Rev.	Data	Motivo Revisione	Preparato da Referente Schema/Direttore/ Resp. SGQ	Verificato da Presidente CSI/ Resp SGQ / Direttore/ Resp. Tecnico	Approvato da A.U. Direttore/ Presidente
09	25/09/2023	Aggiornamento leggi e norme (nuove versioni)	A. Rampazzo	C. D'Aquaro	D. Gilormo
08	07/04/2022	Modifiche a seguito di analisi documentale	V. Mazza	C. D'Aquaro	D. Gilormo
07	19/11/2019	Modifica Logo	V. Guzzo	R. De Pari	D. Gilormo
06	27/08/2018	• Inseriti requisiti per la certificazione con integrazione secondo le linee guida ISO/IEC 270XX (come da circolare Tecnica Accredia n. 02/2018) para 4.2 • Eliminata verifica CSI	S. Ronchi/ R. De Pari	V. Guzzo	R. De Pari
05	25/10/2017	Modificato para 4.1 per i requisiti minimi in termini di Esperienza complessiva e di audit da svolgere; revisione generale per correzione refusi	S. Ronchi/ R. De Pari	F. Banfi	R. De Pari
04	11/02/2015	Modificata da "EA" a "IAF" la denominazione dei Settori merceologici.	S. Ronchi R. De Pari	F. Banfi	R. De Pari
03	01/09/2014	Inserite Note 2 e 3 in para 4.1. Modifiche a seguito di commenti Accredia Cap. 2: Modificati riferimenti/aggiunte alcune norme Cap. 10: Aggiunte 2 leggi applicabili	S. Ronchi R. De Pari	F. Banfi	R. De Pari
02	03/01/2014	Modificata ragione sociale	S. Ronchi R. De Pari	E. Stanghellini	R. De Pari
01	11/01/2010	Inseriti alcuni chiarimenti nel paragrafo 4.1	S. Ronchi R. De Pari	E. Stanghellini	G. Mattana
00	01/09/2009	Completa revisione e nuova numerazione	S. Ronchi R. De Pari	E. Stanghellini	G. Mattana

AICQ SICEV S.r.l.

INDICE

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 la Sicurezza delle Informazioni, 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 la Sicurezza delle Informazioni 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

2.2 Documenti applicabili

- Manuale del Sistema di Gestione per la Qualità di AICQ SICEV e relative Procedure
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27001:2013 + (Cor 1:2014 e Cor 2:2015): Information technology -- Security techniques -- Information security management systems – Requirements
- ACCREDIA Dipartimento DC – Circolare Tecnica N° 15/2023
- ACCREDIA Dipartimento DC – Circolare Tecnica N° 02/2018
- ACCREDIA Dipartimento DC – Circolare Tecnica N° 01/2019

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 EN ISO 19011:2018 Linee guida per gli audit dei sistemi di gestione
- ISO/IEC 27000:2016 - Information technology - Security techniques - Information security management systems – Overview and vocabulary
- ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security management
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls
- ISO/IEC 27003:2017 - Information technology -- Security techniques -- Information security management system implementation guidance
- ISO/IEC 27004:2016 - Information technology -- Security techniques -- Information security management – Measurement
- ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks
- ISO/IEC 27006:2015 - Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27006:2015/Amd 1:2020 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems — Amendment 1
- ISO/IEC 27007:2020 -Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

AICQ SICEV S.r.l.

- ISO/IEC TS 27008:2019 Information technology — Security techniques — Guidelines for the assessment of information security controls
- Line guida per la protezione delle informazioni in ambiti specifici, quali ad esempio:
    - ISO/IEC 27011:2016 Information technology -- Security techniques -- Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organization;
    - ISO/IEC 27013:2015 ""Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
    - ISO/IEC 27017:2015 "Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services";
    - ISO/IEC 27018:2019 (Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors);
    - ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity;
    - ISO 27799:2016 Health informatics -- Information security management in health using ISO/IEC 27002;
    - ISO/IEC TR 27019:2013 Information technology -- Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.
    - Ecc.
- 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
- CobiT - Control Objectives for Information and related Technology (ISACA)

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.

3 DEFINIZIONI E ACRONIMI

Per le definizioni valgono quelle riportate nelle norme UNI EN ISO 19011, ISO/IEC 27000 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:

A.U. – Amministrazione Unico
CSI – Comitato di Sorveglianza dell'Imparzialità
RGVI – Responsabile del Gruppo di Verifica Ispettiva
V.I. – Verifica Ispettiva (Audit)
VSSI – Valutatore del Sistema di Gestione per la Sicurezza delle Informazioni

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

- VSSI – Valutatore di Sistemi di Gestione per la Sicurezza delle Informazioni
- VSSI RGVI – Responsabile Gruppo di Valutazione di Sistemi di Gestione per la Sicurezza delle Informazioni

AICQ SICEV S.r.l.

4. REQUISITI SPECIFICI PER LA CERTIFICAZIONE DEI VALUTATORI (VSGSI) E DEI RESPONSABILI DEI GRUPPI DI VERIFICA (VSGSI RGVI) DI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI (SGSI)

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	**VSGSI** (da VSG di altro Schema a VSGSI - Nota 3)	**VSGSI RGVI** (da RGVI di altro Schema a VSGSI RGVI – Nota 4)
Grado di istruzione	Grado minimo: istruzione secondaria di secondo grado	
Esperienza di lavoro specifica in ambito Sicurezza delle Informazioni	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 27001 (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 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.	In aggiunta a quanto previsto per VSGSI: 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). 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.	

AICQ SICEV S.r.l.

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 per la Sicurezza delle Informazioni.

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 può essere certificato VSSI 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 SSI completi (di cui almeno 1 di 2ª o 3ª parte) per almeno 6 giorni nel ruolo di VSSI condotti sotto la direzione di un RGVI certificato o qualificato, oppure 5 audit di SSI 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 può essere certificato VSSI 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 SSI 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 SSI 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.

4.2 Requisiti addizionali per il riconoscimento delle competenze in ambiti specifici

In materia di Sicurezza delle Informazioni, 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.
La certificazione di un Valutatore (VSSI) o di Responsabile del Gruppo di Valutazione (VSSI-RGVI) dei Sistemi di Gestione per la Sicurezza delle Informazioni a fronte della norma ISO/IEC 27001:2013 può essere estesa anche ad una di queste linee guida ISO/IEC 270XX, come integrazione alla certificazione delle competenze a fronte della norna ISO/IEC 27001.

Detta integrazione può essere richiesta contestualmente alla certificazione delle competenze a fronte della norna ISO/IEC 27001 o anche successivamente, in fase di rinnovo della certificazione o di estensione della stessa,

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 della linea guida ISO/IEC 270XX applicabile 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, sulla linea guida specifica, OPPURE formulazione da parte della commissione esaminatrice, di un numero

AICQ SICEV S.r.l.

adeguato di domande correlate all'ambito specifico, in aggiunta all'esame di certificazione per VSSI / VSI-RGVI
- Esperienza lavorativa o consulenziale nello specifico ambito (relativo alla linea guida ISO/IEC 270XX) 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, sulla linea guida specifica, 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 alla linea guida ISO/IEC 270XX) 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

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.

- VSSI o VSSI RGVI già certificati secondo altri schemi di certificazione di AICQ SICEV (es: Qualità, Ambiente, Salute e Sicurezza).
  In questi casi, ma solo per un periodo di tempo limitato dall'entrata in vigore del presente regolamento, (periodo definito con il CSI e inserito nel documento AICQ SICEV "Casi particolari per certificazione/rinnovo certificazione competenze"), 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
    - Formazione e addestramento

AICQ SICEV S.r.l.

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

- VSSI o VSSI RGVI già certificati da altri OdC di personale accreditati, o riconosciuti a livello internazionale.

- VSSI di grande esperienza professionale cosi definita:
  - almeno 6 anni di esperienza lavorativa in Sistemi di Gestione per la Sicurezza delle Informazioni;
  - 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 per la Sicurezza delle Informazioni 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 la Sicurezza delle Informazioni 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 della Sicurezza delle Informazioni viene riconosciuta come sostitutiva di un anno di esperienza lavorativa specifica.

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

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:

A) affinché venga rinnovata la certificazione della competenza il VSSI 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 VSSI 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.

AICQ SICEV S.r.l.

5. MATERIE DI ESAME

5.1 Modalità di esame

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

5.2 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 Sicurezza delle Informazioni

1.1 Principi fondamentali di gestione (Basic Management)

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

1.2 Principi di Gestione dei Sistemi per la Sicurezza delle Informazioni:

- L'importanza ed efficacia di un Sistema di Gestione della Sicurezza delle Informazioni nelle Organizzazioni, tenendo conto anche degli aspetti economici e di efficienza, della missione e delle strategie aziendali;
- Uso dei principi di gestione delle Sicurezza delle Informazioni;
- Il ruolo dei ISMS managers (CSO, Security Officer, ITC Security Managers …) , requisiti funzionali e posizione nell'organizzazione.
- Compatibilità con altri Sistemi di Gestione.

Ed in particolare:

- Sistemi di gestione basati sul Quality Management.
- Criteri di Auditing Interno per l'ICT Security.
- Gestione della configurazione.
- Gestione delle risorse umane per la Security – consapevolezza.
- Organizzazione dei Sistemi Informativi: ruoli, responsabilità, possibili incompatibilità e segregazione negli incarichi ICT.
- Gestione delle modifiche ai Sistemi Informativi.
- Risk Analysis e Risk Assessment.
- 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.
- Sistemi di controllo interno ed elementi di Corporate Governance.
- Rischi per la Security delle Informazioni nella gestione della catena di fornitura.
- Gestione della Security nell'outsourcing ICT.

1.3 Concetti:

Fondamenti di Security, Sicurezza delle Informazioni, Sistemi ITC e Networking, gestione e miglioramento dei processi di Sicurezza, l'SGSI (o ISMS) e le verifiche (auditing).
In particolare:

- Elementi base dell'ICT, dei concetti di sistema e delle reti.
- Fondamentali della Security.
- Criteri di classificazione dei dati trattati.
- Controllo accesso fisico e logico.

AICQ SICEV S.r.l.

- Protezione delle informazioni ed elementi di crittografia.
- Firma elettronica, digitale.
- Virus, Worms, Programmi maligni in genere, Prodotti e tecniche di prevenzione e di contrasto.
- Cybersecurity, Cyber Crime, Hacking
- Business Continuity, Disaster Recovery e Crisis Management.
- Vulnerability Assessment, Penetration tests e relativi aspetti legali.
- ISO 15408/ITSEC limitatamente alla struttura e ai contenuti del Traguardo di Sicurezza (Security Target) e al formalismo utilizzato per la definizione dei requisiti funzionali
- Rischi per l'ICT Security nel Commercio Elettronico e per l'EDI (Elettronic Data Interchange).
- Rischi per l'ICT Security nella Posta Elettronica.
- Rischi per l'ICT Security nelle operazioni bancarie o di trading remote.
- Rischi di ICT Security nei sistemi di gestione integrati ERP.
- Rischi per l'ICT Security nei Sistemi di supporto alle decisioni (DSS).

1.4 Politica della Sicurezza delle Informazioni:

Sicurezza delle Informazioni come professione e come compito della gestione, gestione attraverso gli obiettivi della Sicurezza delle Informazioni, standardizzazione, reporting e rendiconto e formulazione della politica per la Sicurezza delle Informazioni.

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 della Sicurezza delle Informazioni, obiettivi della Sicurezza delle Informazioni;
- 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 Sicurezza delle Informazioni:

2.1 Organizzazione

Organizzazione delle deleghe delle responsabilità e coordinamento dei compiti. Compiti e posizione del Comitato della Sicurezza, Security Management, Security Team e ruolo del personale della Sicurezza delle Informazioni.

2.2 Meccanismo di coordinamento:

Obiettivi, struttura, procedure e comitati, documentazione del sistema di gestione per la Sicurezza delle Informazioni

AICQ SICEV S.r.l.

2.3 Verifica (auditing):
Verifiche e revisione dell'organizzazione della gestione del Sistema di Sicurezza delle Informazioni (ISMS o SGSI), 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 Sicurezza delle Informazioni

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

4.2 Motivazione:
Teorie della motivazione in relazione alla Sicurezza delle Informazioni.

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 Sicurezza delle Informazioni:
Principi e metodi, messa a punto dei gruppi o team per la Gestione della Sicurezza delle Informazioni, 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. Locali sicuri (camere lampertz).
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 (626 …)

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 Sicurezza delle Informazioni e le loro conseguenze.

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'informazione, 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
- Stima
- Campione
- Uso/utilità dei metodi statistici, nelle verifiche per la sicurezza delle informazioni, 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
- 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

AICQ SICEV S.r.l.

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

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 Sicurezza delle Informazioni, 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
- Privacy: 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)
- Linee Guida Edpb – Linee Guida Art.29
- Decreto Legislativo 10 agosto 2018 n.101
  Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)(GU Serie Generale n.205 del 04-09-2018)
- Decreto Legislativo 18 maggio 2018 n. 51
  Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorita' competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonche' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.
- Conoscenze degli aspetti normativi sulla tutela del Segreto di Stato
- 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 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)
- Aspetti legali e normativi legati all'introduzione della Firma Elettronica e della Firma Digitale (d.lgs. 82/2005)
- Decreto legislativo 61/2011, "Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione"; questo D. Lgs. non è mai stato realmente applicato anche in vista del recepimento della Direttiva NIS.
- Decreto legislativo 65/2018, "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione."; questo D. Lgs. è il recepimento della cosiddetta Direttiva NIS (network and information security).
- Lg 4 agosto 2021 n.109 recante "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*"
- *Direttiva (UE) 2022/2555 NIS 2 Network and information Security*
- DPCM n. 131/2020 - Perimetro di Sicurezza Cibernetico
- D.L n.21 15 marzo 2012 Norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché delle attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni
- DPR n. 54/2021 Regolamento recante attuazione dell'articolo 1 comma 6 del decreto legge 21 settembre 2019 n. 105 convertito con modificazioni dalla legge 18 novembre 2019 n. 133. Si tratta della attuazione della legge sul perimetro di sicurezza nazionale cibernetico, successivo ai primi dpcm uno pubblicato in GU il 20 ottobre 2020 relativo ai criteri di identificazione dei soggetti inclusi nel perimetro
- DPCM 15 giugno 2021 - Individuazione delle categorie di beni Sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetico in attuazione dell'articolo 1 , comma 6, lettera a), del decreto legge 21 settembre 2019 n. 105 convertito con modificazioni dalla legge 18 novembre 2019 n. 133
- D.Lgs n.65 2018 Attuazione della direttiva UE 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione
- D.Lgs n.105 2019 Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica
- Regolamento (UE) 2022/2555 relativo alla resilienza operativa digitale per il settore finanziario Digital Operational Resilience Act DORA

10.2 Aspetti normativi

Norme nazionali ed internazionali, accreditamento e certificazione.

AICQ SICEV S.r.l.