Icmq S.p.A. (A Socio Unico)
Società Benefit
Via G. De Castillia, 10 – 20124 Milano
Tel. 02 7015081 – Fax 02 70150854
icmq@icmq.org – www.icmq.it
P.I. 13218350158

PERCORSO FORMATIVO MODULARE

CYBER TRAINING

Dalle 9:00 alle 13:00

Formazione a distanza (FAD)

STRUTTURA DEL CORSO

MODULO A: FONDAMENTI DI CYBER SECURITY	**15 Aprile 2025**	dalle 9:00 alle 13:00
MODULO B: NIS2 READINESS	**16 Aprile 2025**	dalle 9:00 alle 13:00
MODULO C: BUSINESS CONTINUITY AND INCIDENT RESPONSE	**13 Maggio 2025**	dalle 9:00 alle 13:00
MODULO D: AI GOVERNANCE - ISO/IEC 42001:2023	**14 Maggio 2025**	dalle 9:00 alle 13:00

DESTINATARI

Professionisti IT, responsabili sicurezza, manager e personale operativo di ambito IT/ Security/ Compliance coinvolti nell'implementazione di programmi di cybersecurity.

ATTESTATI E CREDITI FORMATIVI

Verrà rilasciato un attestato di frequenza e saranno riconosciuti **4 crediti formativi** per ogni modulo, validi per il mantenimento della certificazione **Professionisti della Security UNI 10459, DPO Data Protection Officer UNI 11697** al superamento del test di valutazione.

RELATORI

Daniele BAUDONE

Laureato in Informatica collabora con aziende e società di consulenza, in qualità di Business Unit Director, Consulente Cyber Security, Chief Information Security Officer, GRC Director svolgendo attività manageriali e consulenziali, di business development e di consulenza direzionale e tecnica. Ha avviato e diretto team di ICT security in aziende multinazionali hi-tech/cloud, garantendo una gestione efficace della sicurezza informatica che ne ha supportato con successo gli obiettivi e la crescita. Referente Senior in Scuola Internazionale Etica & Sicurezza per tutte i servizi di consulenza e formazione dell'area.

PRESENTAZIONE MODULO A - FONDAMENTI DI CYBER SECURITY

La cybersecurity non è solo un aspetto tecnico, ma un fattore strategico essenziale per la protezione del business. Il corso "Fondamenti di Cyber Security" offre una panoramica operativa per trasformare la sicurezza informatica da adempimento a leva competitiva. Progettato per professionisti IT, responsabili sicurezza e compliance, il percorso unisce teoria e pratica in 4 ore intensive, con focus su rischi digitali, controlli tecnologici e framework normativi. Attraverso simulazioni guidate, analisi di scenari reali e strumenti come SIEM, EDR e crittografia, i partecipanti impareranno a valutare vulnerabilità, implementare piani di remediation e integrare modelli ISO 27001/NIST. Un'occasione per acquisire competenze trasversali su threat intelligence, gestione incidenti e compliance GDPR/DORA, con un approccio concreto alla costruzione di sistemi resilienti.

OBIETTIVI MODULO A

I partecipanti acquisiranno strumenti operativi per:

- Identificare i rischi cyber nel contesto organizzativo
- Impostare e valutare controlli di sicurezza efficaci
- Applicare framework normativi (ISO 27000, NIST CSF, GDPR)
- Gestire incidenti e rafforzare la resilienza aziendale
- Integrare tecnologie come SIEM, EDR e crittografia

PROGRAMMA MODULO A

Introduzione alla Cybersecurity

- Sfide attuali e impatto business
- Asset informativi e classificazione dati
- Threat intelligence e scenario normativo (GDPR, NIS 2, DORA)

Controlli di Sicurezza e Tecnologie

- Strumenti avanzati: EDR, SIEM, firewall di nuova generazione
- Crittografia e Data Loss Prevention
- Vulnerability Assessment/Penetration Test

Governance e Framework

- ISO/IEC 27000 e NIST Cybersecurity Framework
- Modelli di maturity e Security Operation Center (SOC)
- Disaster Recovery e Business Continuity

Case Study Applicativo

- Analisi di un caso studio
- Definizione baseline sicurezza
- Piano di remediation per vulnerabilità critiche

TEST FINALE DI VALUTAZIONE DELL'APPRENDIMENTO

PRESENTAZIONE MODULO B - NIS2 READINESS

La Direttiva NIS 2 rappresenta una svolta normativa che trasforma la cybersecurity da adempimento a pilastro strategico. Questo corso intensivo di 4 ore fornisce una roadmap operativa per implementare i requisiti della direttiva, gestire i rischi digitali e trasformare la conformità in vantaggio competitivo. Attraverso simulazioni pratiche e analisi di casi reali, i partecipanti impareranno a costruire un piano di adeguamento efficace, integrare controlli avanzati e mitigare le sanzioni per il management.

OBIETTIVI MODULO B

Al termine del percorso, i partecipanti saranno in grado di:

- Interpretare obblighi legali e opportunità della NIS 2
- Progettare un piano strategico di compliance con roadmap chiare
- Implementare controlli su supply chain, gestione incidenti e continuità operativa
- Documentare processi secondo standard auditabili

PROGRAMMA MODULO B

Quadro Normativo e Governance

- Requisiti chiave NIS 2 e perimetro di applicazione
- Definizione politica di sicurezza di alto livello
- Modelli di governance e responsabilità del management

Gestione del Rischio e Misure di Sicurezza

- Framework per risk assessment e piani di trattamento
- Controlli IAM e protezione supply chain
- Procedure di segnalazione incidenti (tempistiche e SLA)
- Integrazione sicurezza fisica e ambientale

Continuità Operativa e Audit

- Disaster Recovery Plan allineato alla NIS 2
- Programmi di formazione continua per dipendenti
- Audit interni e testing di Incident Response
- Valutazione efficacia controlli e azioni correttive

Case Study e Benefici Strategici

- Simulazione processo di assessment completo
- Analisi costi/benefici dell'adeguamento
- Positioning sicurezza come asset competitive

TEST FINALE DI VALUTAZIONE DELL'APPRENDIMENTO

PRESENTAZIONE MODULO C - BUSINESS CONTINUITY AND INCIDENT RESPONSE

La resilienza organizzativa e la continuità operativa sono fondamentali per garantire la sopravvivenza e il successo delle organizzazioni in un contesto sempre più complesso e vulnerabile. Questo corso intensivo di 4 ore fornisce competenze pratiche per pianificare, implementare e gestire strategie di resilienza, risposta agli incidenti e continuità operativa. Attraverso simulazioni pratiche e un case study realistico, i partecipanti apprenderanno come affrontare eventi critici, garantire l'operatività aziendale e trasformare la sicurezza in un vantaggio competitivo.

OBIETTIVI MODULO C

Al termine del corso, i partecipanti saranno in grado di:

- Definire strategie di continuità operativa e resilienza per garantire l'operatività anche in condizioni avverse.
- Condurre un'analisi del rischio e una Business Impact Analysis (BIA) per identificare processi critici.
- Implementare piani BCM, BCP, DRP e IRP seguendo standard come ISO 22301 e NIST SP 800-34.
- Gestire efficacemente gli incidenti di sicurezza applicando workflow strutturati e livelli di gravità.

PROGRAMMA MODULO C

Introduzione alla Continuità Operativa e Resilienza

- Definizione di continuità operativa (BC) e resilienza organizzativa.
- Correlazioni tra Business Continuity e Business Resilience.
- Approccio strategico alla resilienza: aspetti chiave e metodologia.
- Cyber Resilience: differenze tra cybersecurity e cyber resilience.

Analisi del Rischio e Pianificazione della Continuità Operativa

- Analisi delle minacce, scenari di rischio e possibili impatti.
- Business Impact Analysis (BIA): obiettivi, fasi e metriche.
- Pianificazione della continuità operativa (BCP): framework ISO 22301 e NIST SP 800-34.
- Strategie di mitigazione degli impatti: Disaster Recovery Plan (DRP).

Gestione degli Incidenti

- Frameworks per la risposta agli incidenti: politiche, monitoring, logging.
- Incident Response Workflow: livelli di gravità degli incidenti.
- Struttura dell'Incident Response Team (IRT) e del CSIRT.
- Requisiti per infrastrutture critiche secondo la direttiva NIS 2.

Simulazione Pratica: Case Study su Continuità Operativa

- Simulazione di gestione di un incidente significativo con attivazione delle procedure BCM/IRP.
- Valutazione dell'efficacia delle strategie adottate.
- Analisi costi/benefici delle misure implementate.

TEST FINALE DI VALUTAZIONE DELL'APPRENDIMENTO

PRESENTAZIONE MODULO D - AI GOVERNANCE - ISO/IEC 42001:2023

Con la crescente diffusione dell'Intelligenza Artificiale (AI) e l'attenzione dei regolatori su sicurezza, etica e privacy, è fondamentale adottare un approccio strutturato alla governance dell'AI. Il corso "AI Governance - ISO/IEC 42001:2023" offre una panoramica completa su come gestire i rischi, garantire la conformità alle normative e integrare la cybersecurity nella governance dell'AI. Questo corso intensivo di 4 ore fornisce strumenti pratici per comprendere e applicare lo standard ISO/IEC 42001:2023, il Regolamento Europeo AI Act e framework di gestione del rischio come il NIST AI RMF. Attraverso esempi concreti e best practice, i partecipanti acquisiranno competenze strategiche per costruire un framework efficace di AI governance che bilanci sicurezza, trasparenza ed etica.

OBIETTIVI MODULO D

Al termine del corso, i partecipanti saranno in grado di:

- Comprendere le implicazioni normative dello EU AI Act.
- Applicare lo standard ISO/IEC 42001:2023 per la governance dell'AI.
- Identificare e mitigare i rischi legati all'uso dell'AI.
- Integrare la cybersecurity nella gestione dell'AI seguendo le linee guida ENISA e NIST.
- Costruire un framework personalizzato per l'AI governance ottimizzando sicurezza e conformità.

PROGRAMMA MODULO D

Introduzione alla Governance dell'Intelligenza Artificiale

- Importanza della governance dell'AI: sicurezza, etica e trasparenza.
- Principali sfide legate alla gestione dell'AI.
- Panorama dei rischi associati all'intelligenza artificiale.

Normative e Framework di Riferimento

- Regolamento Europeo AI Act: requisiti principali e implicazioni.
- ISO/IEC 42001:2023: struttura e applicazione dello standard.
- NIST AI Risk Management Framework: gestione dei rischi nell'AI.
- ENISA Framework for AI Good Cybersecurity Practices (FAICP).

Cybersecurity Integrata nella Governance dell'AI

- Correlazione tra AI governance e framework di cybersecurity (ISO/IEC 27001:2022).
- Best practice per sviluppatori e utilizzatori di AI.
- Strumenti pratici per garantire la sicurezza nell'adozione dell'AI.

Costruzione di un Framework Personalizzato per l'AI Governance

- Strumenti operativi per supportare lo sviluppo della governance (es. AWS Cloud Adoption Framework for AI).
- Simulazione pratica: progettazione di un framework su misura per la propria organizzazione.
- Valutazione costi/benefici delle misure implementate.

Scheda di Iscrizione

CORSO DI FORMAZIONE

CYBER TRAINING

Codice Corso **CYBER_042025**

Date corso **MODULARE – 15 e 16 Aprile 13 e 14 Maggio 2025**

Cognome e Nome*			
Società		***Attività Società***	
Posizione Aziendale			
Indirizzo (via , città , prov, cap)*			
Telefono *		***Cell****	
e-mail*		***P.IVA / C.F.****	
Tipologia Cliente	Business Unit CERSA ☐	ICMQ ☐	ALTRO ☐
Professionista Certificato	☐ Security Uni 10459 ☐ Perito Liquidatore Uni 11628 ☐ Altro _____		

** dati anagrafici della persona che si iscrive al corso*

Dati per intestazione fattura

Il partecipante al corso inoltra la presente richiesta come:

☐ **PRIVATO** per la fatturazione saranno utilizzati i dati sopra indicati ☐ **AZIENDA** compilare i campi sottostanti

Ragione sociale							
C.F.		P.IVA					
Via		Città		Prov.		Cap	
Cell.		Cell. Az.					
Ref. amministrativo							
e- mail - recapito fatture		Mail PEC					
CODICE UNIVOCO		Eventuale n° d'ordine di Acquisto					
☐ Ente Pubblico		☐ Operazione soggetta alla scissione dei pagamenti- Art.17 Ter DPR 633/72 – Split Payment					
Indicare numero c.i.g.:							
Allegare ordine di Acquisto:							

TARIFFA

VOCE	SELEZIONARE MODULI	LISTINO		QUOTA CLIENTI CERSA/ICMQ	
1 Modulo (4 ore)	☐A ☐B ☐C ☐D	€ 300,00 + IVA	☐	€ 250,00 + IVA	☐
2 Moduli (8 ore)	☐A ☐B ☐C ☐D	€ 450,00 + IVA	☐	€ 400,00 + IVA	☐
3 Moduli (12 ore)	☐A ☐B ☐C ☐D	€ 650,00 + IVA	☐	€ 600,00 + IVA	☐
4 Moduli (16 ore)		€ 800,00 + IVA	☐	€ 750,00 + IVA	☐

Modalità di pagamento:

Bonifico Bancario anticipato all'atto dell'iscrizione: **ICMQ S.p.A.** IT91P 05387 01636 000042161048 - BPER BANCA (**nella causale indicare il nominativo del discente e codice del corso**)

Inviare scheda di iscrizione tramite: e-mail: **formazionecersa@icmq.org**

Iscrivendosi al corso ed apponendo timbro e firma sulla presente scheda di iscrizione si prende atto e si accettano le condizioni presenti nel Regolamento e Condizioni di fornitura dei servizi di formazione riportate nella pagina successiva

Data di iscrizione	***Timbro e Firma***
_____/___/_____	

Modalità FAD (Formazione a Distanza)

Informativa UE 2016/679 riguardante l'utilizzo dei dati personali è disponibile su https://www.icmq.it/privacy/privacy-policy.php

SERVIZI DI FORMAZIONE
Regolamento e condizioni generali

Oggetto
Oggetto delle presenti condizioni generali è la fornitura da parte di ICMQ S.p.A. di corsi di formazione come descritti nei documenti di presentazione degli stessi a favore di Terzi (Clienti)

Iscrizione ai Corsi
Al raggiungimento del numero minimo di partecipanti previsto verrà inviata una conferma d'iscrizione tramite e-mail. L'iscrizione ai corsi si intende perfezionata alla ricezione del pagamento del corso e successiva conferma da parte di ICMQ S.p.A.

Sede e date dei corsi
I corsi si terranno nelle date e nelle località riportate nei documenti di presentazione dei corsi. ICMQ S.p.A. potrà in ogni momento comunicare eventuali variazioni relative alla sede o alle date dei corsi.

Diritto di recesso
In caso di disdetta, inviata per iscritto entro 5 giorni lavorativi dalla data di iscrizione, la quota versata sarà interamente restituita. Resta inteso che nessun recesso potrà essere esercitato oltre i termini suddetti e che pertanto qualsiasi successiva rinuncia alla partecipazione non darà diritto ad alcun rimborso della quota di iscrizione versata. E' ammessa, in qualsiasi momento, la sostituzione del partecipante.

Obbligo di frequenza e condizioni per il rilascio degli attestati
I corsisti devono attenersi agli orari prestabiliti e frequentare le sessioni previste dal programma, altresì sono tenuti a firmare quotidianamente un registro di presenza predisposto da ICMQ S.p.A. nel quale sono indicate le eventuali ore di assenza, che devono essere preventivamente autorizzate dal docente.

Corso Completo 40 ore - Auditor di terza parte
Le assenze non dovranno avere una durata superiore a 4 ore consecutive nell'arco della stessa giornata e comunque fino ad un massimo di 8 ore nell'ambito della durata complessiva del corso. Le assenze non sono consentite per le prove d'esame.

Corso 24 ore - Auditor interno/ Corso 24 ore - Upgrade
Le assenze non dovranno avere una durata superiore a 2 ore consecutive nell'arco della stessa giornata e comunque fino ad un massimo di 4 ore nell'ambito della durata complessiva del corso. Le assenze non sono consentite per le prove d'esame.

Corso 8 ore
Le assenze non dovranno avere una durata superiore a 1 ora nell'ambito della durata complessiva del corso. Le assenze non sono consentite per i test.

Corso 4 ore
Non sono consentite assenze.

Nel caso in cui vengano superati tali limiti non sarà possibile sostenere l'esame finale e pertanto verrà rilasciato solo un attestato di frequenza; in ogni caso il partecipante non avrà diritto al rimborso della quota versata per l'intero corso.

Il rilascio dell'attestato di qualifica è subordinato al superamento dei relativi esami.
N.B. Il corso non prevede tirocini, stage e affiancamenti.

Reclami
Il partecipante al corso che non è soddisfatto del servizio offerto può presentare reclamo a ICMQ S.p.A.
Per Reclamo si intende: la segnalazione di una insoddisfazione relativa alla qualità dell'iniziativa corsuale e/o modalità con cui essa si è svolta.
ICMQ S.p.A. conferma il ricevimento del reclamo entro 5 giorni lavorativi dalla sua ricezione.
Il reclamo è esaminato dalla direzione di ICMQ S.p.A. che decide in merito alla sua fondatezza disponendo, se necessario, ulteriori accertamenti. Le decisioni della direzione in merito al reclamo sono comunicate al partecipante.
I tempi per l'accertamento delle cause che hanno determinato il reclamo e quindi la risposta al reclamante dipenderanno dalla tipologia e complessità dello stesso. Le conclusioni sono comunicate al reclamante al termine del processo di istruttoria. Le spese relative al reclamo sono a carico del partecipante richiedente, fatto salvo il caso di accoglimento del reclamo stesso.

Ricorsi
Il partecipante che ritiene ingiusto un provvedimento di ICMQ S.p.A. può presentare entro 10 gg. dal ricevimento del provvedimento medesimo, un motivato ricorso finalizzato alla sua revoca. Il ricorso è esaminato dalla direzione di ICMQ S.p.A. che decide in merito alla sua fondatezza disponendo, se necessario, ulteriori accertamenti. Le decisioni della direzione in merito al reclamo sono comunicate al partecipante mediante comunicazione con avviso di ricevimento.

Rinvio e cancellazione dei corsi
ICMQ S.p.A. si riserva il diritto di annullare o rinviare i corsi, dandone comunicazione scritta al Cliente tramite fax o e-mail. I corrispettivi eventualmente già percepiti da ICMQ S.p.A. saranno restituiti al cliente o d'accordo con lo stesso, saranno imputati come pagamento anticipato per eventuale iscrizione a corsi in date successive.

Quote d'iscrizione
A fronte dell'iscrizione dei partecipanti ai corsi, il Cliente è tenuto al pagamento delle quote d'iscrizione previste dai documenti di presentazione dei corsi, oltre all'IVA. Le quote individuali comprendono, se non diversamente indicato: partecipazione al corso, materiale didattico in formato elettronico, attestato di partecipazione o superamento esami. Le spese per il vitto e l'alloggio dei partecipanti non sono comprese.

Fatturazione e pagamenti
I corrispettivi dovuti dal Cliente, imposte e tasse incluse, devono essere versati anticipatamente all'atto dell'iscrizione. La fatturazione avverrà a quietanza.

Foro competente
Per qualsiasi controversia il foro competente è quello di Milano.