

GIOVEDÌ 17 SETTEMBRE 2026 - ORE 17:00

BUSINESS MASTER

Cyber Security & Artificial Intelligence Risk Compliance Manager

Chiarimenti e approfondimenti



Marco CIAMPI - CEO @ITHUM

Stefania PESCE - Training & PC Operations Manager Italia @DNV



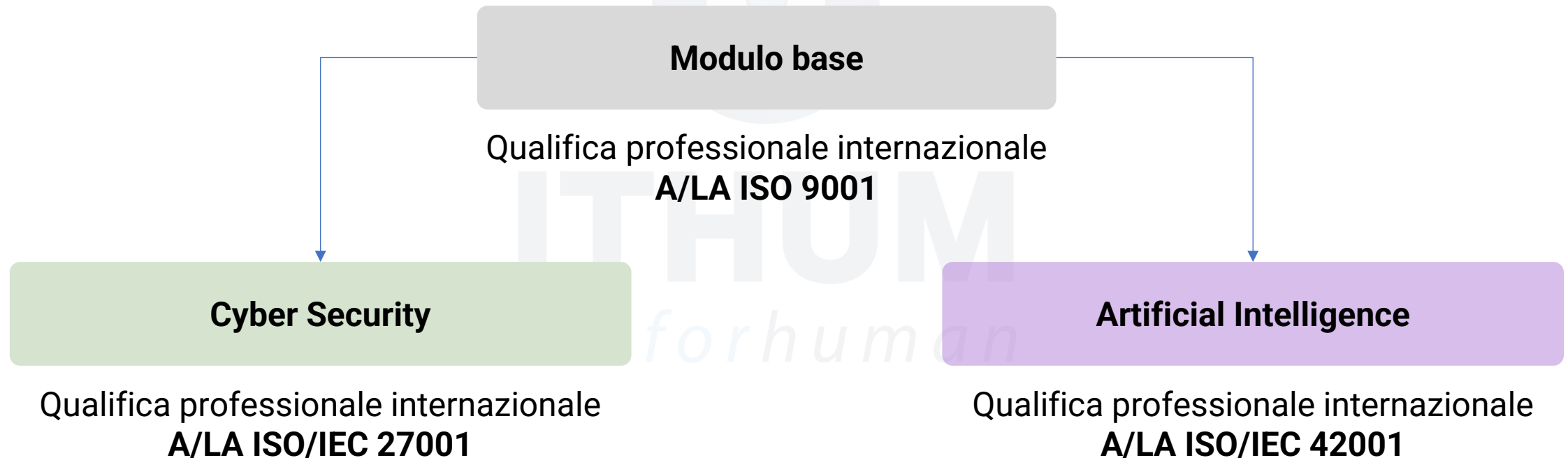
Descrizione

BUSINESS MASTER CYBER SECURITY & ARTIFICIAL INTELLIGENCE RISK COMPLIANCE MANAGER

ha l'obiettivo di **formare professionisti** per **governare in modo integrato** i rischi tecnologici, la conformità normativa e i sistemi di gestione, in un contesto caratterizzato da **minacce cyber sempre più evolute** e da un'accelerazione nell'adozione **dell'Intelligenza Artificiale** senza precedenti

Programma

- ✓ **8-12 ore**/settimana di formazione
- ✓ **martedì/giovedì** e/o **venerdì**
- ✓ **solo mattina** (9:00-13:00) o **giornata intera** (9:00-18:00)



La durata complessiva del Master è di circa **22 settimane** (sia per CS che per AI, che per la combo)

Percorso BASE (fine ottobre / fine gennaio)

Modulo	Descrizione	Ore	Docenti	Date	Ora
Normativa 1	Contesto e normativa di riferimento con particolare focus su NIS2 (e DORA), GDPR, Perimetro Sicurezza Cibernetica 🕒	16	Flavio Marangi, Stefano Aterno, Andrea Cabras (ITHUM)	mar 20/10/2026 ven 23/10/2026 mar 27/10/2026 ven 30/10/2026	9:00-13:00
Tecniche di Audit	UNI EN ISO 19011:2026 e UNI CEI EN ISO/IEC 17021	16	Paolo Scavino (DNV)	ven 6/11/2026 ven 13/11/2026	9:00-18:00
Quality Management System	A/LA UNI EN ISO 9001:2026*	24	Marco Caruso (DNV)	ven 20/11/2026 ven 27/11/2026 ven 4/12/2026 [Ex]	9:00-18:00
Information Security Management System	Norma A/LA ISO/IEC 27001:2022* 🕒 (1° gg del corso A/LA)	8	Fabrizio Cirilli (ITHUM)	ven 11/12/2026	9:00-18:00
Normativa 2	Cybersecurity Act; CER; Cyber-Resilience Act; AI Act – leggi nazionali associate	8	Gregorio Alteri (DNV)	ven 18/12/2026	9:00-18:00
Governance del Rischio	UNI/ISO 31000:2018 e altri standard di Risk Assessment & Governance 🕒	16	Antonio Mauro (ITHUM)	mar 12/01/2027 ven 15/01/2027 mar 19/01/2027 ven 22/01/2027	9:00-13:00
ISO/IEC 27090 Cybersecurity – Artificial Intelligence	ISO/IEC 27090 Cybersecurity Expert per Artificial Intelligence (Guidance for addressing security threats and compromises to artificial intelligence systems) 🕒	8	Fabrizio Cirilli (ITHUM)	ven 29/01/2027	9:00-18:00

Percorso CYBER SECURITY (febbraio / inizio aprile)

Modulo	Descrizione	Ore	Docenti	Data	Ora
Information Security Management System	A/LA ISO/IEC 27001:2022 e ISO/IEC 27002* (2°+3° gg del corso A/LA)	16	Fabrizio Cirilli (DNV)	ven 05/02/2027 ven 12/02/2027 [Ex]	9:00-18:00
Governance del Rischio	UNI/ISO 27005 e Risk Assessment & Management Ⓞ	4	Antonio Mauro (ITHUM)	ven 19/02/2027	9:00-13:00
Incident Management	ISO/IEC 27035 Ⓞ	4	Antonio Mauro (ITHUM)	ven 26/02/2027	9:00-13:00
Cyber-Resilience	Gestione della Continuità Operativa/IT continuity/ IT Resilience Ⓞ	16	Francesco Capparelli, Gerardo Giso (ITHUM)	mar 02/03/2027 (C) ven 05/03/2027 (G) mar 09/03/2027 (C) ven 12/03/2027 (G)	9:00-13:00
Integrazione ISMS/NIST	Uni/Pdr 174	8	Gabriele Picchi (DNV)	ven 19/03/2027	9:00-18:00
IoT Security (Standard ETSI)	ETSI EN 303 645; ETSI TS 103 701	8	Fabrizio Cirilli (DNV)	ven 02/04/2027	9:00-18:00
Project Work	Presentazione e discussione finale Project Work	8	Fabrizio Cirilli (DNV)	ven 09/04/2027	9:00-18:00

Percorso ARTIFICIAL INTELLIGENCE (febbraio / inizio aprile)

Modulo	Descrizione	Ore	Docenti	Data	Ora
Standard ISO su AI	Standard di riferimento per la Gestione dell'Intelligenza Artificiale (ISO/IEC 22989, ISO/IEC 5338, ISO/IEC 5259-2, ISO/IEC 38507, ISO/IEC 24027) Ⓢ	8	Fabrizio Cirilli (ITHUM)	gio 04/02/2027 gio 11/02/2027	9:00-13:00
AI Management System	ISO/IEC 42001:2023* Ⓢ	24	Alessio Aresta (ITHUM)	gio 18/02/2027 gio 25/02/2027 gio 04/03/2027 gio 11/03/2027 [Ex]	9:00-18:00 9:00-18:00 9:00-13:00 9:00-13:00
Gestione del Rischio nell'utilizzo di AI	ISO/IEC 42005, ISO/IEC 23894	24	Fabrizio Cirilli (DNV)	gio 18/03/2027 gio 25/03/2027 gio 01/04/2027	9:00-18:00
Project Work	Presentazione e discussione finale Project Work Ⓢ	8	Alessio Aresta (ITHUM)	gio 08/04/2027	9:00-18:00

Benefit e servizi di cortesia

Oltre alle lezioni frontali e ai materiali didattici, il percorso include anche servizi di cortesia:

- **Testimonianze aziendali**
- **Simulazione** di Audit aziendali
- **Networking meeting con manager DNV:** Roma – Milano – Bologna
- Accesso annuale a **diversi corsi in self-study asincrono** su Cyber Security e Artificial Intelligence (Cisco, LPI, EC-Council, NDG, CompTIA, OpenEDG)
- Accesso gratuito ed esclusivo alla **suite di autovalutazione DNV**
- **Accesso a Lumina™** per le informazioni aggregate su performance del sistema di gestione delle aziende certificate DNV

Finalità del percorso

- ☐ sviluppare un **profilo professionale strategico**
- ☐ lavorare (o aspirare a lavorare) in ambiti **IT, risk management, audit, compliance o sistemi di gestione e ampliare competenze**
- ☐ **affrontare sfide** introdotte da **NIS2, DORA, Cyber Resilience Act e AI Act**
- ☐ acquisire **visione completa** (competenze tecniche, metodologie di governance del rischio e approccio manageriale)
- ☐ **diventare un punto di riferimento in azienda** per valutare rischi, implementare controlli e garantire la conformità
- ☐ costruire un **percorso professionalizzante mirato e distintivo**
- ☐ in cerca di **formazione professionale concreta**, orientata al **business** e subito applicabile, supportata da **esperti di settore**
- ☐ vuoi **rafforzare il tuo profilo professionale** con competenze sempre più richieste dal mercato per guidare trasformazione digitale in modo sicuro e conforme
- ☐ Inserimento nelle **community CS e AI** per condividere passione e relazioni professionali

Requisiti di partecipazione

La partecipazione è consigliata a chi abbia maturato esperienza aziendale e proattività verso miglioramento continuo, oltre a curiosità e interesse nel settore della sicurezza delle informazioni e dell'intelligenza artificiale.

Non sono previsti particolari requisiti di accesso, se non:

- Superamento del questionario d'ingresso (Propedeutico ai corsi AICQ SICEV)
- Diploma di istruzione secondaria superiore o titolo superiore

Modalità di iscrizione



E' possibile **manifestare interesse** con **pre-iscrizione**, non vincolante!

- Manifestazione interesse a master.dnv@ithum.it
- Colloquio profilazione e orientamento professionale (prerequisiti, motivazione, efficacia potenziale)
- Sottoscrizione ordine sul [portale DNV](#)
- Test ingresso (e-mail di DNV - Ufficio Training)
- Superamento test ingresso = pre-iscrizione ufficiale al Master
- Pagamento*

È possibile concordare soluzioni di pagamento personalizzate in base alle esigenze



La conferma del Master avviene al raggiungimento del numero minimo dei partecipanti, entro 20 gg prima dell'inizio delle lezioni.



La **rinuncia** dell'iscritto a partecipare al corso di formazione in seguito alla conferma dell'attivazione del Master da parte di DNV **non dà diritto al rimborso, nemmeno parziale**, della quota di iscrizione e **non esonera** il Cliente dall'adempimento dell'obbligo di **pagamento della quota di iscrizione** non ancora corrisposta.

Prezzi PROMO

Modulo Base

Prezzo lancio*: **€3.950** (invece di €5.820)

Percorso Cyber Security

Prezzo lancio*: **€5.950** (invece di €9.480)

Percorso Artificial Intelligence

Prezzo lancio*: **€5.950** (invece di €9.480)

Percorso completo (Base + Cyber + AI)

Prezzo lancio*: **€7.850** (invece di €12.855)

****IVA esclusa***

Il mestiere di Auditor

evidenze, rischio e giudizio professionale

Un audit di terza parte è un processo sistematico, indipendente e documentato: raccoglie evidenze oggettive e le valuta rispetto a criteri definiti.

Cosa significa fare audit di terza parte

- 1 Criteri**
scope, norme, requisiti e obiettivi del programma
- 2 Evidenze**
interviste, osservazioni, documenti e campionamenti verificabili
- 3 Conclusioni**
valutazione imparziale: conformità, rischi, opportunità e follow-up

La competenza dell'auditor

- Tecnica e settore**
standard, contesto e processi ICT
- Metodo di audit**
interviste, campionamento, evidenze tracciabili
- Comportamento**
integrità, riservatezza, indipendenza
- Sviluppo continuo**
formazione, esperienza e feedback

ISO 19011 principi guida

integrità
presentazione
imparziale
dovuta cura
professionale
riservatezza
indipendenza
approccio basato
su evidenze
approccio basato
sul rischio

Contatti ITHUM

master.dnv@ithum.it

FORMAZIONE

Michela Allegretti (Punto di Contatto)
m.allegretti@ithum.it – 06 2158915

Pamela Solitario (Coordinamento didattico-operativo)
p.solitario@ithum.com

Marco Ciampi (Coordinamento generale)
m.ciampi@ithum.it – 393 9428200

AMMINISTRAZIONE

Monica De Luca
m.deluca@ithum.it – 06 86726329

Contatti DNV

DELIVERY

Giada Raccuglia
(Calendario docenti – Piattaforma gestione corsi LMS)
giada.mariagrazia.raccuglia@dnv.com – 342 0113532

Maria Elena Germondani
(Sito – Promozioni - Piattaforma gestione corsi LMS)
maria.elena.germondani@dnv.com – 347 0633561

Stefania Pesce (Operation Manager)
stefania.pesce@dnv.com – 346 0810502

SALES

Daniele Federicis
daniele.federicis@dnv.com – 348 2320348

Q&A



I nostri Webinar

Webinar precedente

21/07/2026



The poster features the ITHUM logo at the top left and the DNV logo at the top right, with the text "In partnership with" between them. Below the ITHUM logo, it says "MARTEDÌ 21 LUGLIO 2026 - ORE 17:30". The main title is "BUSINESS MASTER Cyber Security & Artificial Intelligence Risk Compliance Manager". Below the title, the speakers are listed: Marco CIAMPI - CEO @ITHUM, Fabrizio CIRILLI - docente del Master, Gregorio ALTERI - ICT New Services Development Senior Specialist @DNV, and Stefania PESCE - Training & PC Operations Manager Italia @DNV. On the right side, there is a circular graphic with a green padlock and circuitry.

ITHUM
it'sforhuman

MARTEDÌ 21 LUGLIO 2026 - ORE 17:30

BUSINESS MASTER
Cyber Security & Artificial Intelligence
Risk Compliance Manager

Marco CIAMPI - CEO @ITHUM
Fabrizio CIRILLI - docente del Master
Gregorio ALTERI - ICT New Services Development Senior Specialist @DNV
Stefania PESCE - Training & PC Operations Manager Italia @DNV

In partnership with

Approved by

DNV

Informazioni, materiali e registrazione: [qui](#)



Fondata nel **2005**
da professionisti ICT e
organizzazione aziendale



Si occupa di
Formazione Certificata
Consulenza Specialistica

Governance



cybersecurity

ICTech



Ha sede a **Roma**
Opera in tutta Italia
ed Europa



Crea **Valore**
con Ecosistemi e Partnership



Artificial Intelligence

- Awareness
- Essentials / Foundation
- Governance:
 - ISO 42001 Artificial Intelligence Management Systems
 - AI Act
- UNI 11621 Professional Profiles:
 - Chief AI Officer
 - AI Consultant
 - AI Prompt Engineer
 - AI Product Manager
 - AI Security Specialist
 - AI Supervisor
 - ISO 27090 AI & Cyber Security

Cyber Security

- IT Security
 - Attacks & Warfare (Red Team)
 - Defence & Analysis (Blue Team)
 - Secure Coding
 - Operation Technology Security
- Governance & Management
- Intelligence & Social
- Investigation & Forensic
- Regulatory Compliance
- Artificial Intelligence

Governance

- Management Systems ISO
 - Information Security
 - Business Continuity,
 - Quality, Anti-Bribery, ICT
 - Artificial Intelligence
 - Environment Social Government
- International Standards
 - Privacy GDPR
 - DPO (Data Protection Officer)
 - Privacy Engineer,
 - Privacy Technician
 - Data Act
 - EuroPrivacy
 - ICT Professional Profiles UNI/EN
 - HR Professional Profiles UNI
- Project Management & Framework
- Management & Soft skills

ICTech

- IT & Operative Systems
- Networking & DevNet
- Cloud & Virtualization
- Containers (Docker, Kubernetes)
- Blockchain
- Development & Programming
- Industry 4.0 (IoT, Big Data, AR)
- Artificial Intelligence
 - Deep Learning
 - Machine Learning



(+39) 06 2158915
(+39) 06 86726329



Via Cristoforo Colombo, 149
00147 Roma (RM) Italy



informazioni@ithum.it



www.ithum.it

