Iniziativa:

"Sessione di Studio" a Roma

Gentili Associati,

Il Consiglio Direttivo è lieto di informarVi che, proseguendo nell'attuazione delle iniziative promosse dall'Associazione Italiana Information Systems Auditors volte al processo di miglioramento, di formazione e informazione dei propri associati, ha organizzato, un incontro che vedrà l'intervento dei seguenti relatori:

Stefano Tassi (ENI)	*Audit alla CyberSecurity: Elementi di complessità di un caso reale*
Serena Valentini (ENI)	
Leonardo Nobile (HPE)	*Cyber Defense – Come essere pronti a minacce di tipo avanzato*
Simone Onofri (HPE)	
Guido Milana (KPMG Advisory S.p.A.)	*Cyber Security Intelligence: approccio e esperienze progettuali per conoscere i potenziali attaccanti della propria organizzazione*

L'incontro avrà luogo a:

Roma, 8 marzo 2017

Presso

Hewlett Packard Enterprise

via Achille Campanile 85, 00144 Roma (RM)

come da agenda allegata.

La modalità di iscrizione alle Sessioni di Studio sarà come sempre gestita attraverso la piattaforma web accessibile al seguente indirizzo:

http://videosessioni.aiea.jed.st/

La sessione, come sempre, è gratuita per gli associati; la partecipazione è estensibile ai non Soci, che intendano associarsi ad AIEA per l'anno 2017:

http://www.aiea.it/html/prima_iscrizione.html

Per aderire alla Sessione di Studio Vi chiediamo perciò di accedere alla piattaforma e confermare la Vostra partecipazione, ***entro e non oltre*** *il*

6 Marzo p.v.

Ricordiamo che la partecipazione all'evento corrisponde sino a ***4*** *ore di credito nell'ambito del CISA/CISM/CGEIT/CRISC Continuing Education (CPE).*

Vi Aspettiamo!

Il Consiglio Direttivo
Milano, Febbraio 2017

Abstract delle relazioni

Stefano Tassi e Simona Valentini (ENI)

- ***Audit alla CyberSecurity: Elementi di complessità di un caso reale***

Negli ultimi anni la tematica della cyber security si è evoluta con rapidità coerentemente con lo sviluppo tecnologico che ha interessato tutti i settori. Tale cambiamento ha caratterizzato la trasformazione significativa dei processi di business aziendali, del sistema di controllo interno e delle relazioni dell'azienda con gli altri attori.
L'auditor, quindi, deve affrontare nuove tematiche e integrarle nelle proprie attività e competenze.
Questo intervento rappresenterà gli elementi di difficoltà rilevati nel corso di un caso pratico di Audit illustrando una sintesi del contesto, dei rischi e degli approcci di auditing utilizzati.

Leonardo Nobile e Simone Onofri (Hewlett Packard Enterprise)

- ***Cyber Defense – Come essere pronti a minacce di tipo avanzato***

"Ci sono solo due tipi di organizzazioni: quelle che sono state già compromesse, e quelle che lo saranno". Così esordisce Robert Mueller - Direttore dell'FBI – nel 2012. È quindi fondamentale capire come queste minacce possono danneggiare la nostra organizzazione e come possiamo proteggerci: non è tanto un problema di "se", ma "quando" ci attaccheranno. L'obiettivo dell'intervento è quello di comprendere anzitutto come operano queste minacce e – tramite esempi e casi reali – come possiamo preparare la nostra organizzazione a resistere agli attacchi e a gestire una compromissione simulando attacchi avanzati - Cyber Attack Simulation.

Guido Milana (KPMG Advisory S.p.A.)

- ***Cyber Security Intelligence: approccio e esperienze progettuali per conoscere i potenziali attaccanti della propria organizzazione***

Nell'ambito della cyber security per prevenire o mitigare potenziali attacchi cyber, oltre ad implementare le tradizionali misure di sicurezza, occorre porre in essere attività di cyber intelligence per acquisire informazioni importanti al fine di adeguare le proprie contromisure.
Non si può immaginare di arginare il fenomeno degli attacchi cyber in modo autonomo ma è auspicabile che anche in Italia si rafforzi la cooperazione tra privati (esempio associazioni di categoria) e con le autorità istituzionali (CERT, Intelligence, Polizia Postale ecc.).
Nell'intervento si condividerà l'approccio e le esperienze progettuali che hanno consentito ad alcune aziende di avviare questo nuovo percorso.

Relatori

Guido Milana

Laureato in Scienze Statistiche ed Economiche è attualmente senior manager di KPMG nell'ambito dei servizi di Information Protection & Business Resilience all'interno del gruppo IT Advisory.
Ha maturato significative esperienze nell'ambito dell'IT Security (disegno ed implementazione di soluzioni di sicurezza, VA-PT in ambito Web e mobile), IT Risk Management (disegno e attivazione dei processi di controllo IT secondo il Cobit 5), IT Compliance (adeguamento dei processi IT per la conformità a normative nazionali ed internazionali).
È certificato CISA, CGEIT, Prince2, ISO/IEC 20000 e 27001, ITIL V.3.

Leonardo Nobile

Security Principal di Hewlett Packard Enterprise, Leonardo ha avviato il proprio percorso professionale presso il Gruppo IBM nel 1994. Nel 1996 entra in Arthur Andersen dove si occupa di IT audit e di IT Governance, Risk & Compliance. Nel 2003 confluisce nel network Deloitte ove assume il ruolo di Director di Deloitte ERS - Enterprise Risk Services.
Dal 2012 al 2016 è stato CIO presso Europa Factor, intermediario finanziario ex art. 106.
Da marzo 2016 ha assunto la carica di Security Principal presso Hewlett Packard Enterprise.
È inoltre proboviro AIEA dal 2009, docente AIEA dal 2005 e trainer accreditato APMG per i corsi e gli esami per la certificazione COBIT 5 Foundation.
È certificato CISA, CISM, Lead Auditor ISO27001, ITIL V3 Foundation, Cobit5 Foundation, Lead Auditor ISO22031, CDP – Consulente della Privacy/Privacy Officer.

Simone Onofri

Cyber Defense Lead di Hewlett Packard Enteprise per l'Europa Sud. Ha cominciato a lavorare come Consulente IT nel 2002, focalizzandosi sempre più sugli aspetti di Sicurezza in ambito Bancario, Governativo-Militare, Telecomunicazioni, Intrattenimento, Retail per Clienti localizzati in zona EMEA.
Collabora con associazioni e organizzazioni come UNINFO – per la stesura della norma relativa ai profili professionali per la sicurezza delle informazioni; OWASP – come uno degli autori della Testing Guide v4 e ISECOM – come uno degli autori della Hackers Highschool.
È qualificato OPSA, ISO 27001 Practitioner, ITIL v3 Service Operation, Cobit 5 Foundation, PRINCE2, AgilePM, P3O Foundaion,CSM, Kanban ACE, DAD Yellow Belt, Six Sigma Yellow Belt e LEGO Serious Play Trained Facilitator.

Stefano Tassi

Laureato in economia e commercio a Roma, ha lavorato per le società di consulenza PricewaterhouseCoopers e successivamente Engineering Management Consulting nelle aree di controllo di gestione, contabilità generale ed analitica. Per due anni ha svolto attività di Audit IT per la Ernst & Young. Dal 2008 lavora in Eni, occupandosi di internal audit, soprattutto in ambito IT. È in possesso della certificazione CISA.

Serena Valentini

Laureata in Ingegneria Civile a Roma, dopo una breve esperienza nell'ufficio gare di un'impresa di costruzioni, nel 2003 ha seguito il master di II° livello in "Governance, sistemi di controllo e auditing" sponsorizzato da Eni Corporate University. Lavora da una decina di anni per la direzione Internal Audit dell'Eni, occupandosi di revisione interna, soprattutto in ambito IT. È certificata CISA.

ISACA
Sistemi informativi: averne fiducia e trarne valore
Capitolo di Milano

PROGRAMMA

14.00	Registrazione dei partecipanti
14.15	Apertura dei lavori
14.30	**Stefano Tassi e Simona Valentini (ENI)** **Audit alla CyberSecurity: Elementi di complessità di un caso reale**
15.30	**Leonardo Nobile e Simone Onofri (Hewlett Packard Enterprise)** **Cyber Defense – Come essere pronti a minacce di tipo avanzato**
16.30	**Coffee Break**
16.45	**Guido Milana (KPMG Advisory S.p.A.)** **Cyber Security Intelligence: approccio e esperienze progettuali per conoscere i potenziali attaccanti della propria organizzazione**
17.45	Dibattito con i relatori
18.15	Termine dei lavori