



Cyber Risk Management with COBIT[®] 5

Be informed, be aware and
be prepared about Cyber Risk



NH Laguna Palace Hotel – Mestre Venezia
venerdì 12 Dicembre 2014



Cyber Risk Management with COBIT® 5

Obiettivi

La Cyber Security è il tema emergente nato per affrontare le nuove forme di criminalità informatica ed in alcuni casi, di guerra cibernetica (cyberwarfare). The Internet of Thing (IoT) cioè la complessità del mondo virtuale che connette oltre 58 miliardi di dispositivi, ha sollevato un problema urgente e persistente che comporta un rapido cambiamento nella percezione del rischio informatico e nel suo trattamento. ISACA ha concentrato i propri sforzi nella realizzazione di molte pubblicazioni sul tema, tra cui la *European Cybersecurity Implementation Series*, per fornire un supporto all'implementazione della sicurezza informatica, in linea con i requisiti europei e le good practise.

Come esempi di gestione dei rischi all'interno del governo di un sistema di controlli interni, saranno anche illustrate:

- l'applicazione della circolare 263 del 27 dicembre 2006 "Nuove disposizioni di vigilanza prudenziale per le banche" di Banca d'Italia
- i benefici nell'implementare l'ISAE (International Standards for Assurance Engagements) 3402 standard di garanzia per il reporting dei controlli nelle service organizations

Programma

09:00-09:15	Registrazione	
09:15-09:30	Welcome	Narduzzo, Salvato
09:30-10:30	La gestione del rischio nell'era digitale	Prof. Giovanni Vaia – Ca' Foscari
10:30-11:00	Cyber Risk Mgmt with COBIT 5	Marco Salvato
11:00-11:15	<i>Coffee Break</i>	-
11:15-11:55	Il Rischio Informatico e le nuove Disposizioni di Vigilanza di Bdl	Luca Lora Lamia - KPMG
11:55 - 12:35	L'attestazione ISAE 3402	Monica Poli – Ernst & Young
12:35-12:45	CSX e conclusione	Dalla Rovere, Narduzzo, Salvato
12:45-14:00	<i>Lunch</i>	

Destinatari

Professionisti nel settore IT, Auditor, IS Auditor, Addetti ai Sistemi Informativi, Responsabile della sicurezza delle informazioni, Consulenti, IT Risk Manager, Responsabile Qualità dei Dati, Responsabile Rischi Operativi, Studenti universitari o Neolaureati.

Organizzazione

Sede: NH Laguna Palace Hotel, Viale Ancona 2, Mestre Venezia

<http://nhlagunapalace.hotelinvenice.com/dove-siamo.html>

Data: Venerdì 12 Dicembre 2014

Orario: 09:00 – 12:45

Partecipazione **gratuita** previa iscrizione soggetta a conferma.

Inviare la scheda di adesione a iscrizioni@isacavenice.org entro il 4 dicembre 2014

CPE

L'evento permette di acquisire **3,5 ore CPE** per le certificazioni CISA, CISM, CGEIT, CRISC, ISO27000LA, CSSP.

ABSTRACT

La gestione del rischio nell'era digitale **Prof. Giovanni Vaia, Ca' Foscari Venezia**

Usate i vostri dati e dei vostri clienti per evolvere la vostra strategia? Usate i vostri dati e dei vostri clienti per generare insights e azioni? Se state cercando di mantenere efficace la vostra Strategia (Digitale) e aggiornata, i dati sono la vostra migliore arma per diverse ragioni. Questo richiede nuove competenze di gestione e nuovi modelli di collaborazione, attraverso nuovi di analisi e gli strumenti per un efficace Business Intelligence, trasferendo le principali applicazioni e prassi nelle aziende, ed una trattazione dello stato dell'arte sullo sviluppo delle architetture a supporto. Ma quali sono i rischi da gestire in queste nuove piattaforme digitali dove stakeholder diversi condividono informazioni e lavorano insieme in un sistema dinamico, senza necessariamente fondersi?

Cyber Risk Management with COBIT 5 **Marco Salvato, ISACA Venice Chapter**

L'intervento illustra i concetti relativi al Cyber Risk ed alla Cyber Security secondo le principali good practise ed associazioni internazionali, fornendo un quadro del materiale prodotto dall'ISACA per supportare le aziende ed i professionisti dell'IT ad affrontare questa tipologia di rischio. In particolare si illustra la collana *European Cybersecurity Implementation Series* e gli altri volumi pubblicati in ambito Cyber Security.

Il Rischio Informatico e le nuove Disposizioni di Vigilanza di Banca d'Italia **Luca Lora Lamia, KPMG**

Il 15° aggiornamento Circ. n. 263 del 27 dicembre 2006 "Nuove disposizioni di vigilanza prudenziale per le Banche" introduce nell'ambito bancario un insieme di previsioni ereditate dalle migliori best practices di IT Governance e IT Security. Il concetto di "Rischio" pervade tutta la normativa in oggetto, a partire dal Cap. 7 dedicato al sistema dei controlli interni in ambito di governo aziendale per poi verticalizzare la propria declinazione in ambito informatico (Cap 8 - Sistema informativo). L'intervento, dopo una breve introduzione del contesto normativo, descrive un approccio all'analisi e alla gestione del rischio informatico che a partire dagli standard di riferimento di settore (es. COBIT, ISO3100, ISO27005) si declina in metodologie e processi conformi ai principi (coinvolgimento vertici aziendali, visione integrata dei rischi, efficienza ed efficacia dei controlli, applicazione delle norme in funzione della dimensione e della complessità operativa) e agli specifici requisiti introdotti dalle disposizioni di vigilanza.

L'attestazione ISAE 3402 **Monica Poli, Ernst & Young**

L'importanza dei controlli sull'efficacia e dei processi di reporting è considerata sempre più critica e la globalizzazione e i cambiamenti di regolamentazione hanno spinto all'emissione dello standard ISAE 3402. L'attestazione ISAE 3402 (International Standard for Assurance Engagements) è la valutazione del sistema dei controlli di organizzazioni che erogano servizi, prevalentemente in ambito IT e amministrativo, ed è rilasciata da Auditor Indipendenti, i quali hanno la responsabilità di valutarne la descrizione, il disegno e l'efficacia, rispetto a best practice di controllo. Tale attestazione è ad uso delle Società che utilizzano i servizi oggetto di verifica e dei loro rispettivi auditors, essendo tali servizi a supporto della produzione dell'informativa contabile e di bilancio. Il principio ISAE 3402 prevede che l'Auditor emetta un'Attestazione sulla descrizione, sul disegno e sull'efficacia dell'effettivo funzionamento del Sistema di Controllo della società, nel periodo di verifica e con riferimento a obiettivi di controllo predefiniti sui processi in oggetto. Obiettivo della relazione sarà, pertanto, descrivere lo standard di attestazione, le tipologie, i suoi scopi, le metodologie utilizzabili, i benefici, i vantaggi attesi e le effettive modalità di applicazione del progetto.

CSX **Rudi Dalla Rovere**

Cyber Security NeXus (CSX): overview del nuovo percorso di certificazione ISACA sulla Cyber Security.

BREVI NOTE PERSONALI SUI RELATORI

Giovanni Vaia – Università Ca' Foscari Venezia

Laureato con lode in Economia Aziendale all'Università di Napoli, è professore aggregato di Economia Aziendale e Global Sourcing presso il Dipartimento di Management dell'Università Ca' Foscari di Venezia, già professore a contratto di gestione dei sistemi informativi presso l'Università di Salerno, e dottore di ricerca in Organizzazione e Tecnologia, è coinvolto attualmente nell'elaborazione di ricerche che si focalizzano sul design organizzativo e in particolare sui Sistemi Informativi e Servizi IT (IT Service Management), Innovazione Digitale, su network governance e outsourcing, governance dei sistemi informativi, IT Outsourcing.

A Ca' Foscari ha fondato e coordina il Digital Enterprise LAB, è fondatore e membro della faculty del Center For Automotive & Mobility Innovation, ed è ideatore e coordinatore del Tavolo di Lavoro permanente su Innovazione, Tecnologia e Sistemi Informativi. E' inoltre membro del comitato di gestione di Edizioni Ca' Foscari. I suoi ultimi lavori sono stati pubblicati su: Management of Information System Quarterly Executive, Journal of Information Technology TC, Economia & Management.

Giovanni è stato menzionato sui principali quotidiani nazionali come il Sole24Ore, Milano e Finanza, Il Corriere della Sera, Il Mattino, e su riviste internazionali specializzate.

E' membro del Consiglio Direttivo di ITSMF Italia www.itsmf.it, dove coordina l'Osservatorio sull'IT Service Management, e ha assunto la carica di Presidente del Chapter Italiano di IAOP (International Association of Outsourcing Professionals®) www.iaop.org. In IAOP è membro della commissione di ricerca internazionale sull'outsourcing.

Marco Salvato - ISACA VENICE Chapter

Marco Salvato CISA, CICM, CGEIT, CRISC, COBIT 5 Foundation, COBIT 5 Approved Trainer, ha maturato un'esperienza nel settore IT superiore ai 30 anni. In passato ha lavorato come consulente e come imprenditore. Svolge attività di formazione per il capitolo in ambito CISA e COBIT 5. Attualmente lavora per Generali Business Solutions e ricopre la carica di vicepresidente dell'ISACA VENICE Chapter.

Luca Lora Lamia - KPMG

Luca Lora Lamia Manager KPMG - Information Risk Management, ha maturato una decennale esperienza in ambito *IT Governance, Risk, Security and Compliance* e in particolare nell'ambito dei sistemi di gestione, nel governo e nella gestione di programmi e progetti di innovazione organizzativa e tecnologica.

Ha acquisito competenze specifiche in ambito IT and Security Risk Management collaborando anche in progetti internazionali legati alla sicurezza delle infrastrutture critiche.

In merito agli adempimenti legati alla conformità alle nuove disposizioni di vigilanza prudenziale per le banche (15° aggiornamento della Circolare n. 263 di Banca d'Italia) gestisce le progettualità di adeguamento normativo per banche e Centri Servizi. Dal gennaio 2014 segue i progetti della Service-Line Information Risk management (IRM) di KPMG Advisory S.p.A. nel Triveneto.

Monica Poli – Ernst & Young

Monica Poli è una manager del dipartimento Risk di Ernst & Young Financial Business Advisors.

Laureata in Economia Aziendale a Cà Foscari, Venezia, nel 2006, si specializza nell'Information Technology grazie ad un master organizzato da H-Farm s.p.a. sui new Media.

Entra in EY nel 2007 e si specializza in IT Risk Assurance per gli Istituti Bancari e Assicurativi, con focus sulle: attività di Information System Audit; Certificazioni ISAE3402, 262, SOXA; attività di rilevazione, analisi e creazione di processi aziendali e del ciclo di formazione di bilancio. E' referente nazionale EY per le attività di Financial Audit IT Integration a livello di Europa, Africa e Middle East.

Vive a Mestre, in provincia di Venezia e opera in tutto il Nord Italia con predominanza nel Nord Est.

Rudi Dalla Rovere – ISACA Venice Chapter

Dalla Rovere Rudi: IT Security Officer per Generali Infrastructure Services, trainer ISACA CISA dal 2011. Si occupa di information security governance, security architecture, IT security testing and auditing.

Scheda di Iscrizione (inviare a ISCRIZIONI@ISACAVENICE.ORG entro 4 DICEMBRE 2014)

Le adesioni saranno accettate fino ad esaurimento dei posti disponibili e saranno confermate con apposita mail.

Evento Cyber Risk Management with COBIT 5 – 12.12.2014 – mattino 9-13

DATI PERSONALI:

Cognome:

Nome:

Indirizzo:

Cap: Città Prov.

Telefono: Cell:

E-mail:

GARANZIE E DIRITTI DELL'INTERESSATO in ottemperanza al D.Lgs. 196/03 "Codice in materia di protezione dei dati personali". I dati personali in possesso dell'Associazione sono direttamente da Lei forniti ovvero acquisiti altrimenti nel rispetto delle disposizioni legislative vigenti e potranno formare oggetto di trattamento per gli scopi amministrativi del presente seminario e/o associativi. Titolare del trattamento è ISACA VENICE CHAPTER che è a disposizione per l'eventuale aggiornamento, rettifica, integrazione o cancellazione.

Data

Firma

SPONSOR E SOSTENITORI DI ISACA VENICE CHAPTER



Sostenitore Platinum



Sponsor Platinum



Sostenitore Platinum

con il patrocinio di



AICA
Associazione Italiana per l'Informatica
ed il Calcolo Automatico





ISACA – Information Systems Audit & Control Association E' una associazione internazionale, indipendente e senza scopo di lucro. Con oltre 100.000 associati in più di 160 Paesi, ISACA (www.isaca.org) è leader mondiale nello sviluppo delle competenze certificate, nella promozione di community professionali e nella formazione nei settori dell'assurance e sicurezza, del governo dell'impresa, della gestione dell'IT e dei rischi e della compliance in ambito IT. Fondata nel 1969, ISACA organizza conferenze internazionali, pubblica l'*ISACA Control Journal*, sviluppa standard internazionali di audit e per il controllo dei sistemi IT, che contribuiscono a facilitare il perseguimento dell'affidabilità e a trarre valore dai sistemi informativi. ISACA attesta l'acquisizione delle competenze e delle conoscenze IT mediante certificazioni riconosciute a livello internazionale quali: CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CGEIT (Certified in the Governance of Enterprise IT) e CRISC (Certified in Risk and Information Systems Control). ISACA aggiorna continuamente il frame work COBIT che assiste i professionisti dell'IT e i manager delle imprese nel far fronte alle proprie responsabilità per quanto attiene l'IT governance e la gestione manageriale, in particolare nell'ambito di assurance, sicurezza, rischio e controllo e a fornire valore al business.

ISACA Venice Chapter E' un'associazione non profit costituita in Venezia nel novembre 2011 da un gruppo di professionisti del Triveneto che operano nel settore della Gestione e del Controllo dei Sistemi Informativi: è il terzo capitolo italiano di ISACA. Riunisce coloro che nell'Italia del Nord Est svolgono attività di Governance, Auditing e Controllo dei Sistemi Informativi promuovendo le competenze e le certificazioni professionali sviluppate da ISACA. L'associazione favorisce lo scambio di esperienze, promuove un processo di sensibilizzazione di tutti i livelli organizzativi aziendali alla necessità di stabilire adeguati criteri di controllo sia di affidabilità dell'organizzazione sia di sicurezza dei sistemi.

