



Sicurezza delle informazioni Come migliorare le proprie competenze



<http://creativecommons.org/licenses/by/4.0/deed.it>

 Cesare Gallotti

Cesare Gallotti

Milano, 3 giugno 2019

Alcune domande

Perché:

- ancora molti parlano di nomina a responsabile del trattamento?
- tanti chiedono di avere l'informativa privacy firmata dal personale?
- molti citano il NIST e il DoD per la cancellazione sicura dei documenti con 35 passaggi anche se le ultime versioni dei loro documenti non lo dicono?
- periodicamente riemerge l'idea di fare valutazioni quantitative per il rischio relativo alla sicurezza delle informazioni?
- auditor e consulenti sono convinti della bontà della valutazione del rischio (informatico o della sicurezza delle informazioni) basata sugli asset?
- in tanti pensano che «approccio agile» vuol dire «approccio senza documenti»?



Alcune risposte

- Gli studi dimostrano che
 - > prediligiamo informazioni in grado di confermare le nostre credenze;
 - > ci concentriamo sulle informazioni negative;
 - > tendiamo ad affidarci agli stereotipi e a imitare la maggioranza.
- E' stato studiato anche il "pensiero veloce", basato sulle scorciatoie mentali.

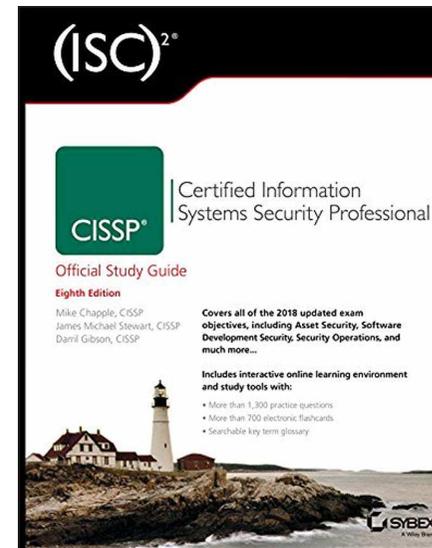


Indice

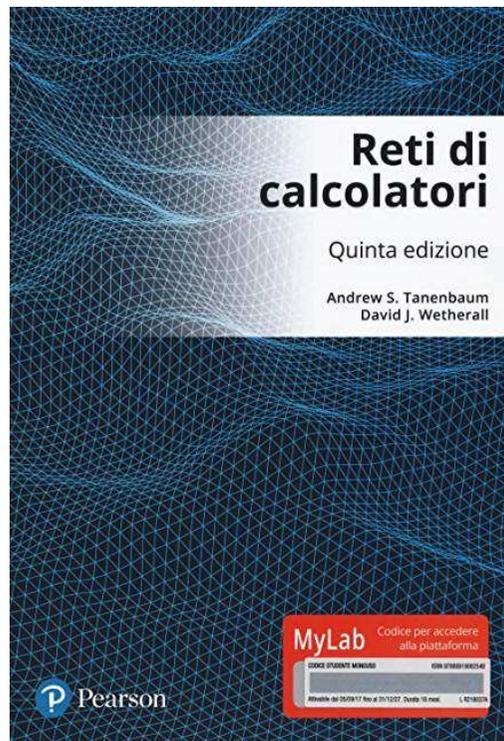
- Tecnologia
- Sistemi di gestione
- Valutazione del rischio
- Normativa
- Newsletter varie



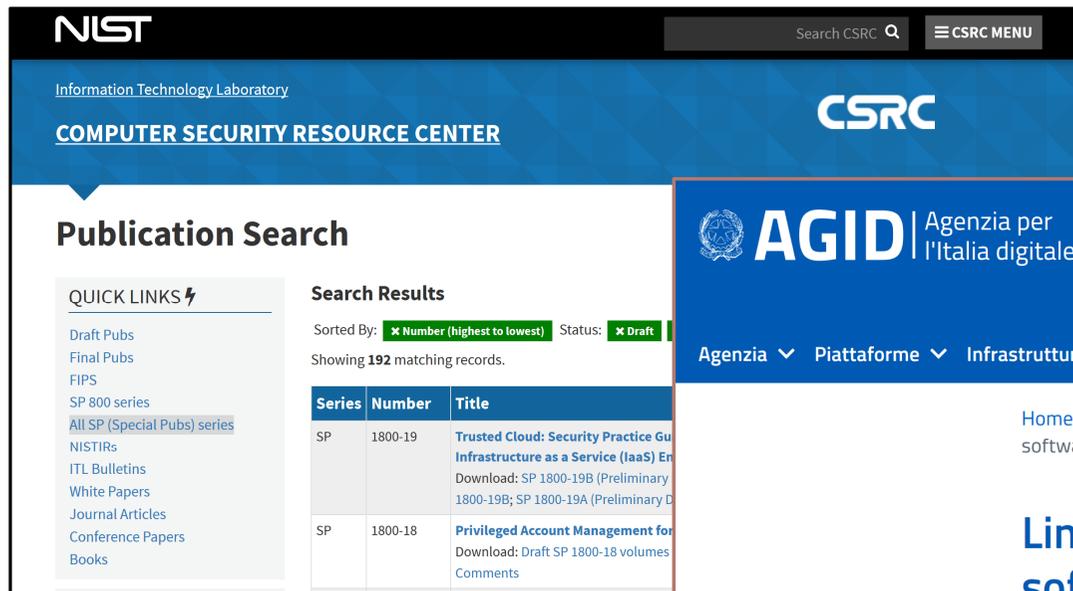
Tecnologia – Per iniziare



Tecnologia – per i teorici



Tecnologia – Tenersi aggiornati – Siti web



NIST Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

Search CSRC CSRC MENU

Publication Search

QUICK LINKS

- Draft Pubs
- Final Pubs
- FIPS
- SP 800 series
- All SP (Special Pubs) series
- NISTIRs
- ITL Bulletins
- White Papers
- Journal Articles
- Conference Papers
- Books

Search Results

Sorted By: **Number (highest to lowest)** Status: **Draft**

Showing 192 matching records.

Series	Number	Title
SP	1800-19	Trusted Cloud: Security Practice Guide for Infrastructure as a Service (IaaS) Environments Download: SP 1800-19B (Preliminary Draft); SP 1800-19A (Preliminary Draft)
SP	1800-18	Privileged Account Management for Cloud Environments Download: Draft SP 1800-18 volumes 1-3



AGID Agenzia per l'Italia digitale

Seguici su

Cerca nel sito

Agenzia Piattaforme Infrastrutture **Sicurezza** Dati Design servizi Linee guida Progetti

Home > Sicurezza > CERT-PA > Linee guida per lo sviluppo del software sicuro

Linee guida per lo sviluppo del software sicuro



Il Consiglio federale MELANI

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI

Pericoli attuali Come mi proteggo? Documentazione Formulario d'annuncio A proposito di MELANI

La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI > Documentazione > Bollettino d'informazione

Bollettino d'informazione

Documentazione

Bollettino d'informazione [Abbonarsi alla newsletter MELANI](#) [Feed RSS](#) [Contenuto](#)

Rapporti



enisa European Union Agency for Network and Information Security

Publications

[ENISA reports](#) [Corporate documents](#) [Cyber security info](#)

[Find publications](#)

Sistemi di gestione – Per iniziare

INTERNATIONAL STANDARD **ISO/IEC 27001**

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

EUROPEAN STANDARD **EN ISO 9001**

NORME EUROPÉENNE

CHE NORM

September 2015

Supersedes EN IS

Quality manage

INTERNATIONAL STANDARD **ISO/IEC 27003**

Second edition
2017-03

Information technology — Security techniques — Information security management systems — Guidance

Technologies de l'information — Techniques de sécurité --Systèmes de management de la sécurité de l'information — Lignes directrices

ALBERTO NEPI

Introduzione al Project Management

Che cos'è, come si applica, tecniche e metodologie

Terza edizione aggiornata e ampliata

The Scrum Guide™

The Definitive Guide to Scrum:
The Rules of the Game

QITIL

ITIL® Foundation
ITIL 4 Edition

AXELOS GLOBAL BEST PRACTICE

ITIL® OFFICIAL PUBLISHER



Valutazione del rischio (i classici)

Carnegie Mellon University Enter

Software Engineering Institute

About ▾ Research and Capabilities ▾ Publications ▾ News and Events ▾

SEI > Publications > Digital Library > Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process

Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process



www.mehari.info

MEHARI 2010

Manuel de référence des Services de Sécurité



European Union Agency for Network and Information Security

TOPICS NEWS PUBLICATIONS EVENTS ⁵

Home > Topics > Threat and Risk Management > Risk Management > Current Risk > RM Inventory > RM/RA Methods

Threat and Risk Management

- > Threat Landscape
- ^ Risk Management
 - ^ Current Risk
 - ^ RM Inventory
 - > Introduction

Inventory of Risk Management / Risk Assessment Methods

ENISA has generated an inventory of Risk Management / Risk Assessment methods. A total 17 methods have been considered. Each method in the inventory has been described through a template. The template used consists of 21 attributes that describe characteristics of a method.



Special Publication 800-30

Risk Management Guide for Information Technology Systems

Recommendations of the National Institute of Standards and Technology

Valutazione del rischio (andare “oltre”)

INTERNATIONAL STANDARD

IEC 60812

First edition
1985

Analysis techniques for system reliability
Procedure for failure mode and effects analysis (FMEA)

NORME INTERNATIONALE INTERNATIONAL STANDARD

Pr

Analyse par arbre de panne (AAP)

Fault tree analysis (FTA)

ROSI Return on Security Investments: un approccio pratico

Come ottenere Commitment sulla Security

NORME INTERNATIONALE INTERNATIONAL STANDARD

CEI IEC 61882

Première édition
First edition
2001-05

Etudes de danger et d'exploitabilité (études HAZOP) – Guide d'application

Hazard and operability studies (HAZOP studies) – Application guide



Valutazione del rischio (ricordare il passato)

CRAMM User Guide

Issue 2.0 January 2001

DESCRIPTION OF AUTOMATED RISK MANAGEMENT PACKAGES THAT NIST/NCSC RISK MANAGEMENT RESEARCH LABORATORY HAVE EXAMINED

Updated March 1991

@RISK

Methodology. Quantitative. @RISK is a 123/Symphony/Excel add-in for risk analysis using Monte Carlo simulation. Probability distributions are added to cells using 30 new probability distribution built-in functions. Carlo or L simulating calculated

Information Systems Security Design Methods: Implications for Information Systems Development

RICHARD BASKERVILLE

School of Management, Binghamton University, Binghamton, New York 13901

The security of information systems is a serious issue because computer abuse is increasing. It is important, therefore, that systems analysts and designers develop expertise in methods for specifying information systems security. The characteristics found in three generations of general information system design methods provide a framework for comparing and understanding current security design methods. These

- Perché il "passato" alcune volte è lontano...



Normativa

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Home L'Autorità Provvedimenti e normativa Attività e documenti Stampa e comunicazione Attività internazionali

Diritti Come tutelare i tuoi dati **Doveri**

Stampa e comunicazione > Newsletter

inserisci chiave di ricerca cerca testo docweb

Newsletter

Stampa PDF Invia per mail Condivisi

FORENSICS GROUP
Legal and Forensics Advisor

Team Scientifico
InCrime

FORENSICS GROUP ▾ PUBBLICAZIONI ▾ AREE TEMATICHE ▾ EVENTI *GD

filodiritto
APPROFONDISCI SEMPRE

24.07.2007 n. 7770 - ISSN 223

ALTALEX

Vuoi fare **pubblicità** su questo sito?
Vuoi **collaborare** con Altalex?

Home Sezioni ▾ Strumenti ▾ **Premium** ▾ Forum

ACQUISTA FORMAZIONE IN AULA FORMAZIONE ON LINE LIBRI E CODICI EBOOK PERIODICI

PROFESSIONI

Non s
altale
Bastano
profilo, s



Newsletter e altro



SANS

Newsletters

SANS NewsBites

SANS NewsBites is a semiweekly high-level executive summary of the computer security during the last week. Each news item is very briefly information, if possible.



Clusit
Associazione Italiana
per la Sicurezza Informatica

Home Sezioni L'associazione Associarsi Formazione Eventi D

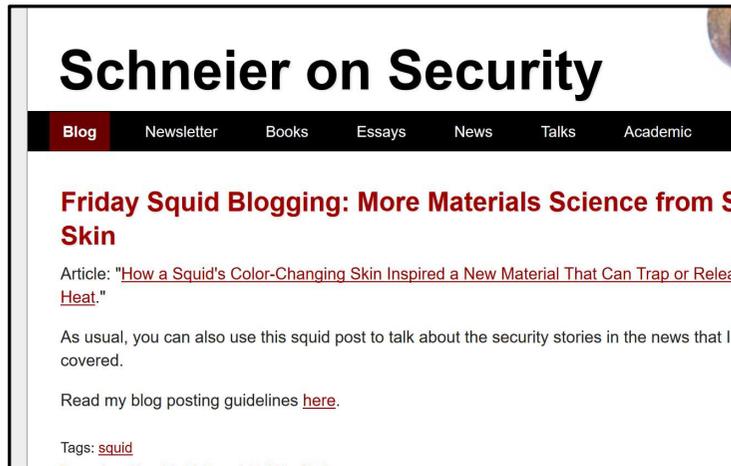
Area Stampa Aree riservate 🔍

Newsletter

✉ [Iscrizione](#) 📅 [Archivi](#)

Iscrizione alla newsletter del CLUSIT

Iscrivendovi alla newsletter CLUSIT riceverete con cadenza mensile inform



Schneier on Security

Blog Newsletter Books Essays News Talks Academic

Friday Squid Blogging: More Materials Science from S Skin

Article: "[How a Squid's Color-Changing Skin Inspired a New Material That Can Trap or Release Heat.](#)"

As usual, you can also use this squid post to talk about the security stories in the news that I haven't covered.

Read my blog posting guidelines [here](#).

Tags: [squid](#)



Powered by DuckDuckGo

blog essays whole site

Subscribe

About Bruce Schneier



Altro ancora



Associazione Italiana
Information Systems Auditors



Ch

Sessioni di studio

Oltre ad interventi mirati e specifici, trattati nel corso del Convegno annuale dei
per tali temi può stimolare la creazione di un su



[Formazione](#) [Eventi](#) [Documenti](#) [Newsletter](#) [Area Stampa](#)

Digital
Forensics
Alumni

Associazione Digital Forensics Alumni

[I Perfezionisti](#) [Associazione](#) [Iscriviti](#) **[Newsletter](#)** [Documenti](#) [Seminari ed eventi](#)

[Open Day](#) [Contatti](#)

Iscrizione

Dubbi

- Seguire i bollettini sulle minacce più diffuse?
- Seguire i rapporti sulle opinioni dei manager in merito ai rischi?
- Approfondire i meccanismi di funzionamento del Garante privacy?
- Approfondire gli ultimi attacchi?
- Tralasciare ogni testo che (oggi) parla di «nomina a responsabile privacy», «visione olistica» e «proattività»?
 - > e quelli che dicono che la sicurezza è un'opportunità?
 - > e quelli che ripetono che la valutazione del rischio inizia dal censimento degli asset?
 - > e quelli che dicono che è possibile (o, addirittura, auspicabile) una valutazione quantitativa del rischio relativo alla sicurezza delle informazioni?





FINE

Web: www.cesaregallotti.it

Blog: blog.cesaregallotti.it

Twitter: [@cesaregallotti](https://twitter.com/cesaregallotti)

