



Information Security nelle Norme Internazionali

SMAU, 19/10/2007

© Fabio Guasconi

at4m 
advanced techniques for management

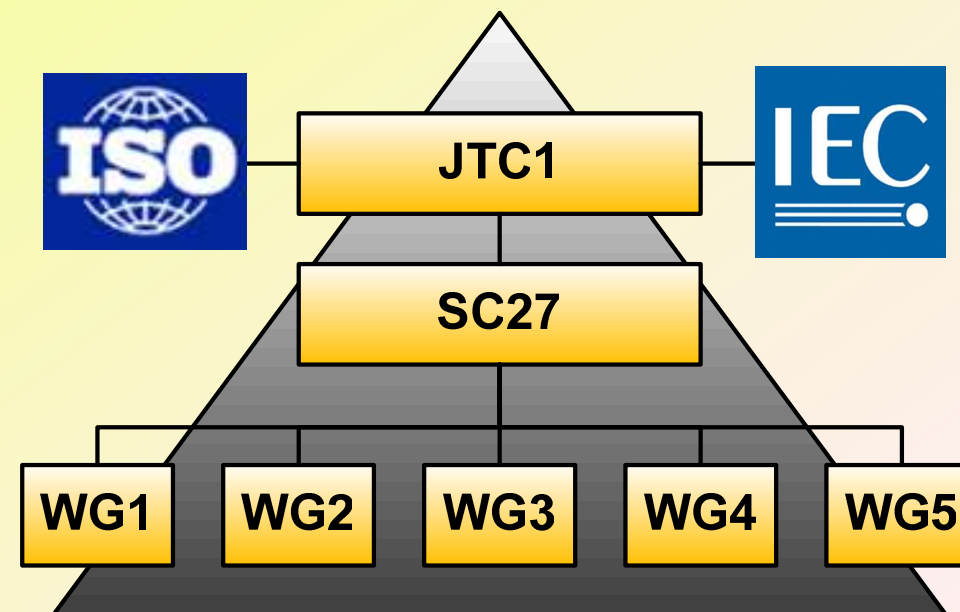
About Me

Consulente per la sicurezza delle informazioni

- Esperto nazionale UNINFO
- Editor della traduzione italiana della 27001
- Consulente su Security Policy, IT Risk Management, Service Management, Business Continuity e Disaster Recovery
- Auditor per lo schema 27001

ISO/IEC JTC1/SC27

(Information technology - Security techniques)



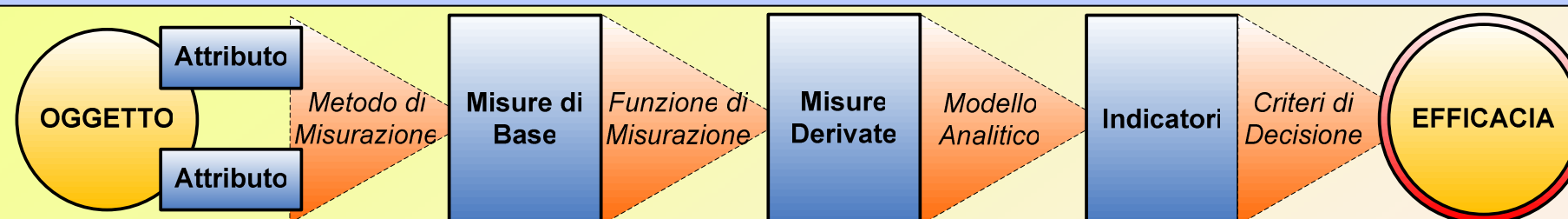
Working Groups SC27

- ▶ **WG1** ISMS Standards
- ▶ **WG2** Security Techniques (Cryptography)
- ▶ **WG3** Security Evaluation Criteria
- ▶ **WG4** Security Controls & Services **NEW!**
- ▶ **WG5** Privacy, Biometric, IAM **NEW!**

La Famiglia 27000

- 27000 2ndCD Overview and vocabulary
- **27001:2005 ISMS requirements**
- **27002:2005 Code of practice for ISM**
- 27003 4thWD ISMS implementation guidance
- 27004 2ndCD Information Security Management Measurements
- 27005 2ndFCD Information Security Risk Management
- **27006:2007 Requirements for bodies providing audit and certification of ISMS**
- 27007 NWI ISMS auditing guidelines
- ...
- 27011 FCD Information Security Management guidelines for telecommunications
- 27031 NWI ICT Readiness for Business Continuity
- 27032 NWI Guidelines for Cybersecurity
- 27033 FCD Network Security
- 27034 NWI Application Security

ISO/IEC 27004



“Guideline”, non “Requirement”

Norma di carattere originale ma fortemente dibattuta, specie dagli americani del NIST

Impostazione ciclica (PDCA), suggerisce la creazione di un **programma** di misurazioni per l'efficacia dei controlli, degli obiettivi e anche dell'intero ISMS

ISO/IEC 27004

Number of privileged accounts / system administration accounts	11.2.2
Number of changes of administrator permissions	11.2.2 11.2.4
Number of detected unauthorized access attempts (firewall)	11.4.6 10.10.2
Number of detected unauthorized access attempts (IDS)	11.4.6

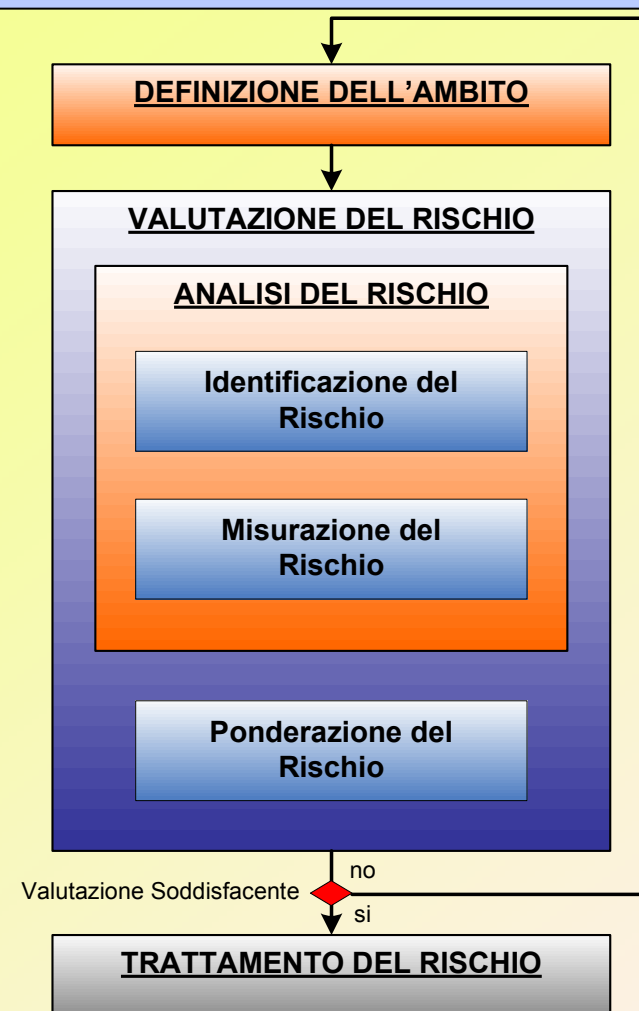
Percentage of false positives (IDS)	Measure Identification	
Number of violations of password policy	Measure Name	Measure Name
Number of password resets	Numerical Identifier	Unique organization-specific numerical identifier
Number of detected malicious software	Control or Control Objective	Control or control objective under measurement.
	Purpose of Measure	Defines the goal of collecting and reporting the measure.
	Reviewer	Person or organizational unit who review that the measure evaluation criteria are appropriate to verify the control effectiveness.

Objects of Measurement and Attributes	
Object of Measurement	The object that is to be measured. Objects may include processes, systems, or system components.
Attributes	Property or characteristic of an object of measurement that can be distinguished quantitatively or qualitatively by human or automated means.

Base Measure Specification	
Base Measures	A base measure is a measure of a single attribute defined by a specified measurement method (e.g., number of trained personnel, number of sites, cumulative cost to date). As data is collected, a value is assigned to a base measure.
Measurement Methods	The logical sequence of operations that define the counting rule to calculate each base measure.
Scale	The ordered set of values or categories that are used in the base measure.

Saggio
degli annex

ISO/IEC 27005



SMAU, 19/10/2007

Altra "Guideline"

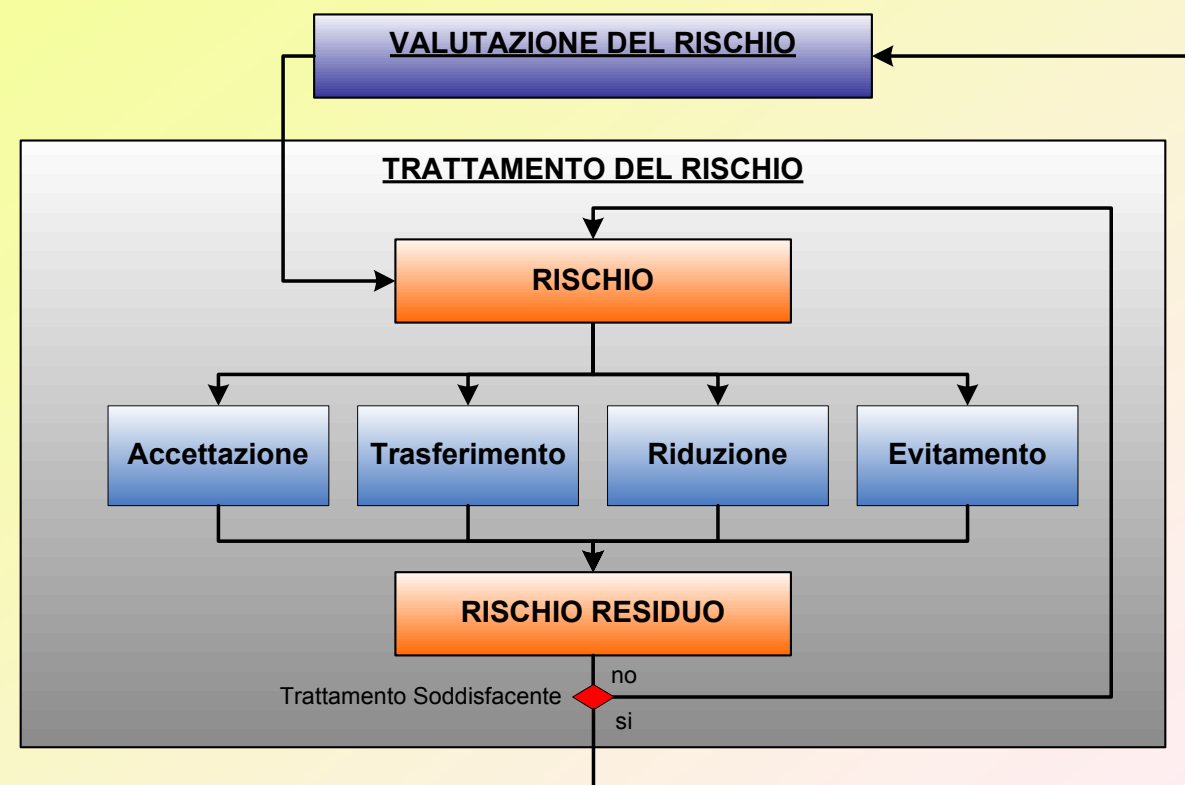
Non originale: ricalca i concetti della vecchia ISO Guide 73 e ne riutilizza la terminologia

Valutazione e Trattamento del Rischio, con **Comunicazione e Monitoraggio** in parallelo

Dettaglio preciso per ogni fase e numerosi esempi negli annex informativi

© Fabio Guasconi

ISO/IEC 27005

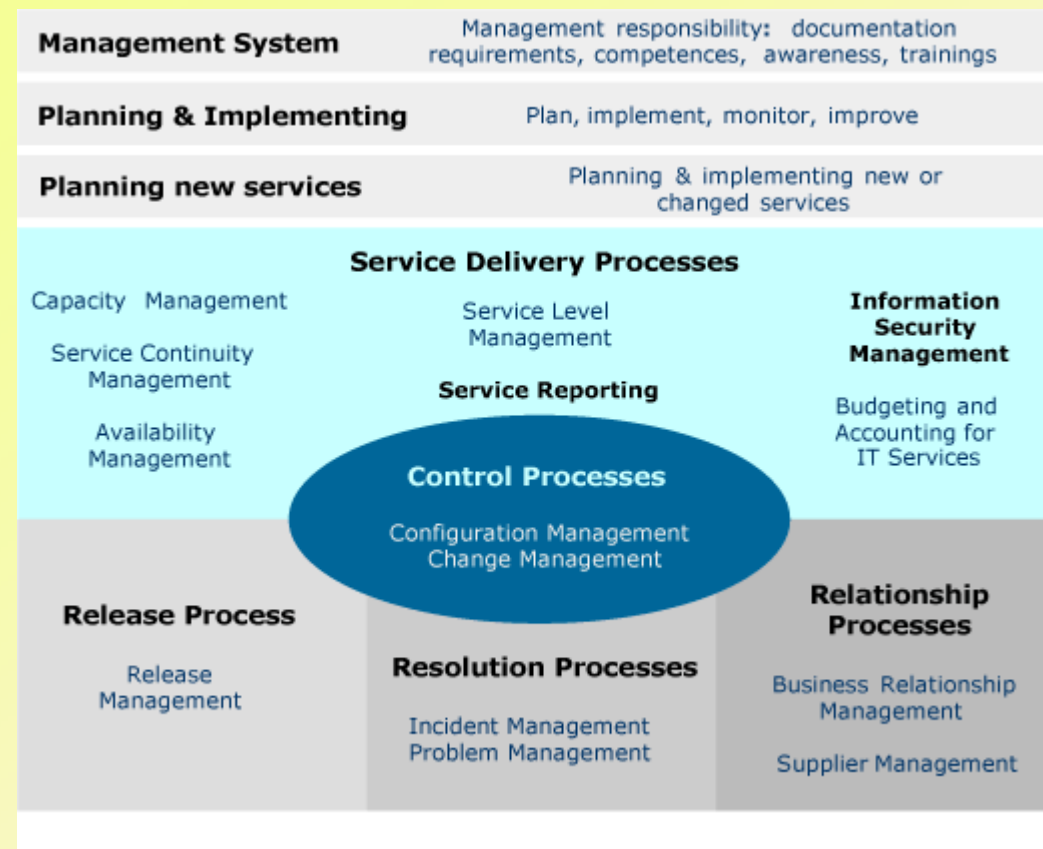


Il **Trattamento** del Rischio è focale per il processo

Telco, BC e Cybercrime

- ▶ **27011** è l'estensione della 27002 (nuovi controlli) tagliata per le organizzazioni del settore telco; fornisce linee guida
- ▶ **27031** inerente agli aspetti legati alla continuità operativa, diviso in 8 parti
- ▶ **27032** cura, con preciso riferimento agli ISP, il lato organizzativo di tematiche tecniche (e.g. anti-spyware), multipart

ISO/IEC 20000 – ITIL(v2)

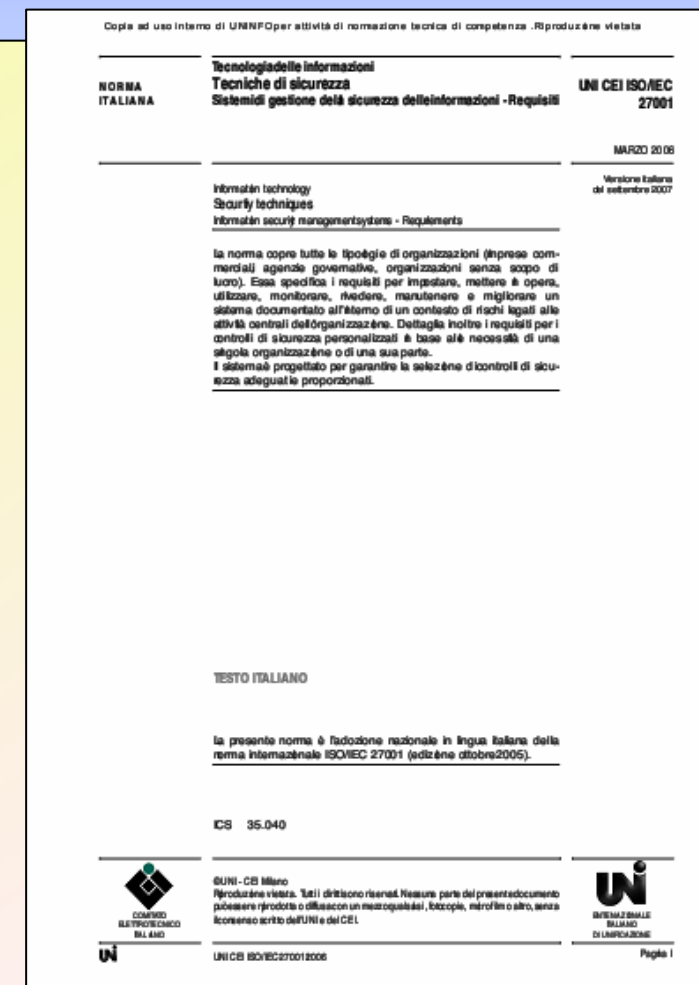


Framework completo per l'**IT Service Management**, integra la gestione della sicurezza, dove è indicata la "vecchia" 17799.

UNI CEI ISO/IEC 27001:2007

Iniziata nei primi mesi del 2006, il GdL UNININFO “Sicurezza delle Informazioni” ha finalmente ricevuto l’approvazione del testo proposto da UNI all’inizio di Ottobre 2007.

La norma è ora disponibile in lingua italiana!!



SMAU, 19/10/2007

© Fabio Guasconi

at4m 
advanced techniques for management

Question time!



Personal cont@ct:
f.guasconi@at4m.eu
329.465.69.30

Corporate websites:
www.at4m.eu – www.sgssi.net