Standard ISO/IEC 270xx

Milano, 10 novembre 2011

Agenda

- Presentazione relatore
- Introduzione agli standard ISO/IEC 27k
- La norma ISO/IEC 27001 in (molto) breve
- La certificazione ISO/IEC 27001
- Gli standard della famiglia ISO/IEC 27k
- Comitati ISO e UNINFO

- Presentazione relatore
- Introduzione agli standard ISO/IEC 27k
- La norma ISO/IEC 27001 in (molto) breve
- La certificazione ISO/IEC 27001
- Gli standard della famiglia ISO/IEC 27k
- Comitati ISO e UNINFO

Cesare Gallotti

- Lead Auditor ISO/IEC 27001 (CEPAS), ISO 9001:2000 (IRCA), ISO/IEC 20000-1 (itSMF); ITIL Expert (Exin); CISA; Computer Forensics (Specializzazione Post Universitaria)
- Esperienze pregresse
  - Consulente, Responsabile di progetti e formatore in ambito ISMS e ITSMS per società di consulenza italiane (Securteam, Intesis, Quint)
  - Lead Auditor e ICT Technical Responsible per DNV Italia (auditing, sviluppo tecnico degli schemi di certificazione collegati agli standard ISO 9001, ISO/IEC 27001 e ISO/IEC 20000-1; sviluppo della relativa formazione)
- Attualmente consulente free-lance:
  - Consulenza in ambito ISMS, QMS, ITSM, Risk Assessment e Privacy
  - Auditor di terza parte per la sicurezza delle informazioni, qualità e dispositivi medici
  - Formatore per corsi LA ISO/IEC 27001, ITIL Foundation e Quality Assurance
  - Attività in Europa, Africa and Asia per clienti di diversi settori di mercato

- Presentazione relatore
- Introduzione agli standard ISO/IEC 27k
- La norma ISO/IEC 27001 in (molto) breve
- La certificazione ISO/IEC 27001
- Gli standard della famiglia ISO/IEC 27k
- Comitati ISO e UNINFO

Standard verificabili vs. linee guida

- Standard verificabile: uno standard con specifiche rispetto alle quali può essere condotto un audit da parte di personale indipendente
- Linee guida: manuali o raccolte di best practices disponibili per una loro selezione al fine di raggiungere un certo obiettivo
- Cosa offre lo standard?
  - > Soluzioni nate dall'esperienza di migliaia di utenti di sistemi di gestione per la sicurezza delle informazioni
  - > Un approccio sistematico per il cambiamento e per il miglioramento (PDCA)
  - > Requisiti focalizzati su pratiche di sicurezza delle informazioni, sui processi collegati, sulle pratiche gestionali e sulle persone coinvolte
  - > Vantaggi: struttura simile agli standard di qualità, ambiente e sicurezza del personale (safety)

ISO/IEC 27001 vs. ISO/IEC 27002

- La ISO/IEC 27001 presenta i *requisiti* (usa il verbo "shall") di un ISMS affinché possa essere certificato.
- I requisiti sono divisi in 2 parti (le appendici B e C sono *informative*):
  - requisiti di sistema (capitoli da 4 a 8)
  - controlli di sicurezza (Annex A)
- La ISO/IEC 27002 è una *linea guida* ("*Code of practice for information security management*", usa il verbo "should") che riporta i controlli di sicurezza della 27001 e li approfondisce. È una sorta di manuale o di linea guida che presenta delle *best practices*.

Cronologia

Linee guida (ISO/IEC 27002)

1995: BS 7799

BS 7799-1:1999

↓

ISO/IEC 17799:2000

ISO/IEC 17799:2005

↓

ISO 27002:2005 (del 2007)

Requisiti (ISO/IEC 27001)

BS 7799-2:1998

BS 7799-2:1999

BS 7799-2:2002

↓

ISO/IEC 27001:2005

- Presentazione relatore
- Introduzione agli standard ISO/IEC 27k
- La norma ISO/IEC 27001 in (molto) breve
- La certificazione ISO/IEC 27001
- Gli standard della famiglia ISO/IEC 27k
- Comitati ISO e UNINFO

Definizioni – Sicurezza delle informazioni

- Informazione: il risultato della raccolta e dell'elaborazione di dati elementari, significativi e utili al processo decisionale. Le informazioni possono essere stampate o scritte su carta, gestite con strumenti informatici, trasmesse via posta o con mezzi elettronici, presentate in film o dette in conversazioni
- Sicurezza delle informazioni: l'attività volta a definire, conseguire e mantenere
  - la riservatezza,
  - l'integrità
  - la disponibilità

  delle informazioni

Definizioni - Sistema di gestione

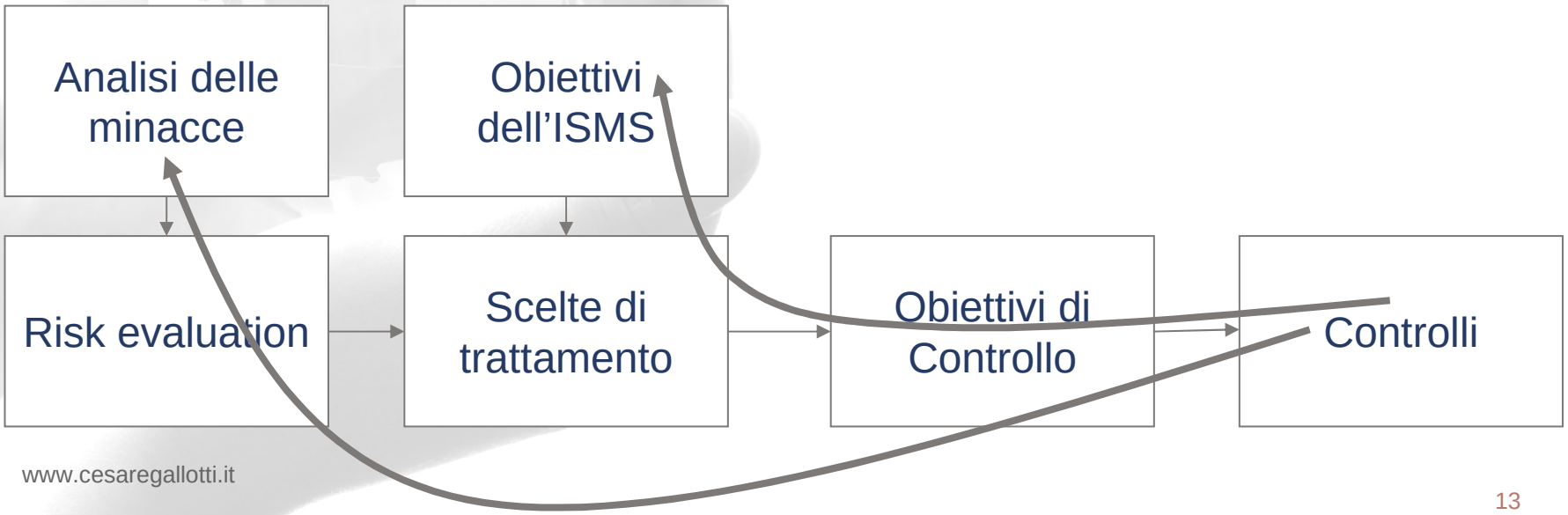
- Sistema (ISO 9000): insieme di elementi tra loro correlati o interagenti
- Sistema di gestione: insieme di politiche, procedure e linee guida e delle risorse ad esse collegate volte a raggiungere gli obiettivi dell'organizzazione (ISO 9000: sistema per stabilire politiche e obiettivi e per raggiungere tali obietti)
- Sistema di gestione per la sicurezza delle informazioni (SGSI): Quella parte del sistema di gestione complessivo, basata su un approccio rivolto al rischio relativo al business, volta a stabilire, attuare, condurre, monitorare, riesaminare, mantenere attivo, aggiornato e migliorare la sicurezza delle informazioni.

I requisiti della ISO/IEC 27001:2005

- Requisiti di sistema:
  - > Stabilire politiche e obiettivi
  - > Condurre il risk assessment e pianificare il trattamento del rischio
  - > Gestire la documentazione e le registrazioni
  - > Gestire le risorse umane
  - > Gestire l'implementazione, l'operatività e la manutenzione dei controlli di sicurezza
  - > Gestire gli acquisti
  - > Gestire le Non Conformità e gli incidenti
  - > Effettuare riesami della Direzione
  - > Condurre audit interni
  - > Elaborare dati sull'efficacia del ISMS
  - > Gestire i processi di miglioramento
- Controlli di sicurezza:
  - > 133 controlli di tipo amministrativo, tecnico, gestionale

Sui controlli

- Le minacce analizzate devono essere collegate ai controlli scelti per contrastarle
- I controlli devono essere correlati alle minacce che contrastano (per dimostrarne l'utilità e l'adeguata robustezza)
- Non è obbligatorio realizzare tutti i controlli. Essi sono descritti in modo generico (nessun "stringente criterio")



I controlli di sicurezza

- A.5 Politica per la sicurezza
- A.6 Organizzazione della sicurezza delle informazioni (organizzazione interna e gestione clienti e fornitori)
- A.7 Gestione degli asset
- A.8 Sicurezza delle risorse umane
- A.9 Sicurezza fisica e ambientale (inclusa manutenzione impianti)
- A.10 Gestione delle comunicazioni e dell'operatività
- A.11 Controllo degli accessi IT
- A.12 Acquisizione, sviluppo e manutenzione dei sistemi informativi
- A.13 Gestione degli incidenti
- A.14 Gestione della continuità operativa
- A.15 Gestione della conformità (a Leggi e procedure)

- Presentazione relatore
- Introduzione agli standard ISO/IEC 27k
- La norma ISO/IEC 27001 in (molto) breve
- La certificazione ISO/IEC 27001
- Gli standard della famiglia ISO/IEC 27k
- Comitati ISO e UNINFO

Il requisito della ISO/IEC 27001

- L'ambito deve essere descritto con i seguenti elementi:
  - caratteristiche del business (prodotti o servizi)
  - organizzazione (organigramma)
  - localizzazione,
  - asset e tecnologia adottata
- E' possibile "ritagliare" con più cura l'ambito del ISMS.

Cosa si può certificare

- Si deve certificare un "ambito" (o "scopo di certificazione") che sia sotto il controllo dell'organizzazione che intende certificarsi.
- L'ambito deve essere descritto con i seguenti elementi:
  - caratteristiche del business (prodotti o servizi)
  - organizzazione (organigramma)
  - localizzazione,
  - asset e tecnologia adottata
- Importante:
  - alcune aziende certificano solo una parte delle loro attività (deve essere controllato il certificato)
  - il certificato non vuol dire che l'azienda è sicura, solo che ha pianificato e realizzato e che mantiene misure di sicurezza coerenti con la propria valutazione del rischio (bisogna quindi chiedere dettagli sulle misure di sicurezza)

Falsi miti

- Sono falsi miti:
  - io sono certificato ISO -> sono al sicuro
  - il mio fornitore è certificato ISO -> è sicuro anche secondo i miei standard, anche se non glieli ho detti
  - ricerco un fornitore ISO -> non ho bisogno di comunicargli i miei requisiti di sicurezza perché tanto lui è sicuro -> non ho neanche bisogno di capire cosa c'è scritto sul suo certificato
  - compro un prodotto ISO (ISO/IEC 15408) o da un fornitore ISO -> il prodotto è sicuro
  - il mio cliente, fornitore o partner è ISO -> tutto ciò che dice è buono e giusto
- Ricordarsi, di fronte a un certificato:
  - leggere di quale azienda si tratta, di quali siti sono coinvolti e quali attività sono coperte
  - chiedere, se necessario, dettagli sulla realizzazione delle misure di sicurezza (p.e. la disponibilità di un sito alternativo e i tempi di ripristino)

L’accreditamento

- “Quis custodiet ipsos custodies?” (o “who watch the watchmen?”, come ci ricorda anche Alan Moore).
- Gli “Organismi di Certificazione” devono essere a loro volta *accreditati*.
- Gli Enti di Accreditamento, uno per ogni Stato, svolgono questo ruolo:
  - regolamentati in Europa dalla EC Regulation 765/08
  - si riconosco reciprocamente attraverso gli accordi EA MLA
  - sono su http://www.european-accreditation.org/content/mla/scopes.htm
  - in Italia è Accredia (www.accredia.it)
- Ovviamente... ci sono anche altri Enti di Accreditamento:
  - al di fuori degli EA MLA, ma che si occupano di certificazioni non sostenute dai membri
  - al di fuori degli EA MLA e che si occupano di certificazioni sostenute dai suoi membri (e quindi non riconosciuti dalla EC Regulation 765/08)

Richiedere un certificato

- In molte gare o richieste di offerta si richiede la certificazione ISO/IEC 27001.
- Cosa chiedere:
  - che la certificazione sia sulla versione in vigore della ISO/IEC 27001, secondo i regolamenti dell'Ente di Accreditamento
  - che la certificazione copra completamente l'ambito oggetto della gara o della richiesta di offerta
  - che i servizi oggetto della gara o dell'offerta vengano erogati dai siti coperti dal certificato (o che questo verrà esteso quanto prima a quei siti)
  - che il certificato sia rilasciato da un Organismo di Certificazione accreditato da un Ente membro degli EA MLA
- L'Italia è piena di esempi di come NON fare un bando (nominano ISO/IEC 17799, BS 7799, vecchie versioni della norma, settori merceologici assurdi; non fanno riferimento all'ambito, ai siti e all'accreditamento).

- Presentazione relatore
- Introduzione agli standard ISO/IEC 27k
- La norma ISO/IEC 27001 in (molto) breve
- La certificazione ISO/IEC 27001
- Gli standard della famiglia ISO/IEC 27k
- Comitati ISO e UNINFO

Standard verificabili vs. linee guida

- Standard verificabile: uno standard con specifiche rispetto alle quali può essere condotto un audit da parte di personale indipendente
- Linee guida: manuali o raccolte di best practices disponibili per una loro selezione al fine di raggiungere un certo obiettivo
- Questa diapositiva è ripetuta per ricordare le due definizioni. Gli standard certificabili sono solo:
  - ISO/IEC 27001
  - ISO/IEC 27006 e ISO/IEC 17021 (solo per gli Organismi di Certificazione)

I fondamentali (versioni a settembre 2011)

- ISO/IEC 27000:2009: Information technology – Security techniques – Information security management systems – Overview and vocabulary (la nuova versione è al 3WD)
- ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements (la nuova versione è al 1CD; c'è chi dice che per fine 2012 sarà emessa)
- ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management (la nuova versione, al 4WD, dovrebbe essere emessa insieme alla 27001)
- ISO/IEC 27006:2007 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems (la nuova versione è al DIS; è in revisione causa pubblicazione ISO/IEC 17021:2011)

Quelle più note (versioni a settembre 2011)

- ISO/IEC 27003:2010 - ISMS Implementation Guidance
- ISO/IEC 27004:2009 – Measurement
- ISO/IEC 27005:2011 – Information Security Risk Management (aggiornata causa ISO 31000:2009 e ISO Guide 73:2009)

Quelle meno note – Pubblicate (a settembre 2011)

- ISO/IEC 27011:2008 - Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27031:2011 - Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27035:2011 - Information technology -- Security techniques – Information security incident management

Quelle meno note in sviluppo (versioni a settembre 2011)

- ISO/IEC 27007 sull'auditing. Ora allo stato di FDIS
- TR ISO/IEC 2008 con linee guida per gli auditor. Pronta per la pubblicazione
- 27010 su "for intersector and inter-organisational communications", ora al 1CD
- 27013 su relazioni tra 27001 e 20000-1, ora al 1CD
- E poi: su governance, sul settore finance, sulla cybersecurity, sulla application security, sull'outsourcing, sulla forensics, eccetera

Altre di interesse (versioni a settembre 2011)

- ISO 31000:2009 - Risk management -- Principles and guidelines
- ISO Guide 73:2009 - Risk management -- Vocabulary
- ISO/IEC 31010:2009 - Risk management -- Risk assessment techniques
- ISO 22301 Societal security -- Preparedness and continuity management systems -- Requirements (stato DIS)
- ISO/PAS 22399:2007 - Societal security - Guideline for incident preparedness and operational continuity management
- ISO/IEC 24762:2008 - Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services

Norme per gli audit (versioni a settembre 2011)

- ISO 19011:2002 (UNI EN ISO 19011:2003) - Guidelines for quality and/or environmental management systems auditing
- ISO/IEC 17021:2011 (UNI CEI EN ISO/IEC 17021:2011) - Conformity assessment -- Requirements for bodies providing audit and certification of management systems

L’indice della nuova 27001 (versione del maggio 2011)

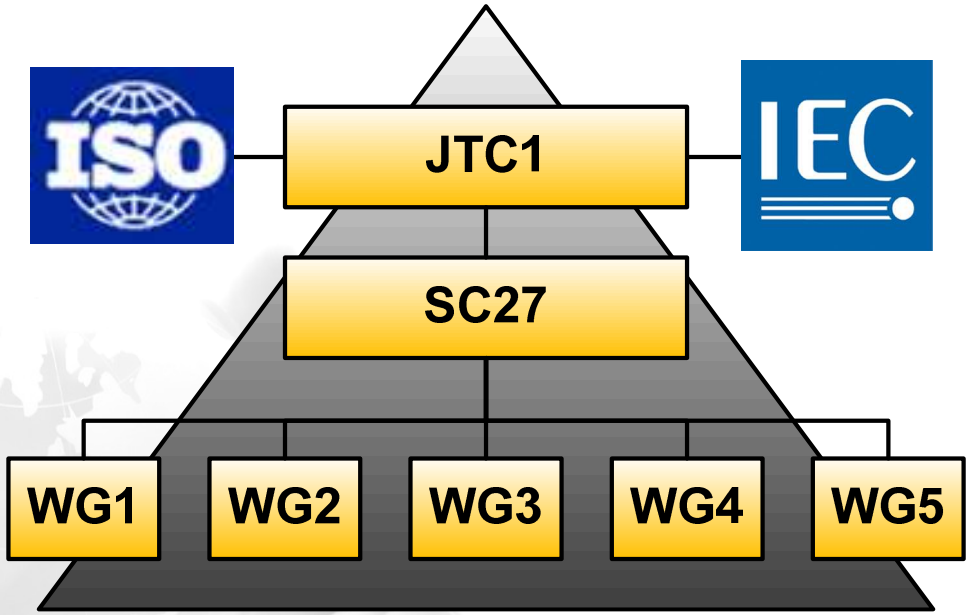
- 0 Introduction
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4.1 Understanding the organization and its context
- 4 Context of the organization
- 5 Leadership
- 6 Planning
- 7 Support
- 8 Operation
- 9 Performance Evaluation
- 10 Improvement
- Annex A (normative) Reference control objectives and controls

- Presentazione relatore
- Introduzione agli standard ISO/IEC 27k
- La norma ISO/IEC 27001 in (molto) breve
- La certificazione ISO/IEC 27001
- Gli standard della famiglia ISO/IEC 27k
- Comitati ISO e UNINFO

UNINFO

- Ente di normazione italiano federato all'UNI
- Settore: tecnologie informatiche
  - Codifica e decodifica video, Sicurezza/Security, Ingegneria del Software, Open Source, Accessibilità, Smart Cards, Biometrica, Sistemi Bancari, E-business, Telematica per i trasporti - ITS, Codifiche - RFID, Applicazioni, Informazioni Geografiche, Telecomunicazioni, Automazione Industriale, Linguaggi, Learning Technologies, Apparecchiature e Supporti, Documenti ed elementi di informazione
- Mantiene contatti con ISO, IEC, CEN, ETSI
- Sito web: www.uninfo.polito.it

ISO/IEC JTC1 SC27



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

GdL Serie ISO/IEC 27000

- Nato il 19 Maggio 2010 con 20 partecipanti tra esperti e aziende
- Rappresenta la **voce italiana ufficiale** ai lavori di normazione
- Sviluppa le tematiche legate agli standard e alla loro applicazione (e.g. relazioni con normativa sulla Privacy)
- Consente l'accesso a tutti i documenti di lavoro della serie 27000
- Legato al più ampio SC27 che segue anche Common Criteria (ISO/IEC 15408), crittografia, privacy e tecniche di sicurezza
- Sito web: http://www.uninfo.polito.it/SC27/SC27_GdL27000.htm

Partecipanti al GdL

Esperti indipendenti

Mauro Bert

Fabrizio Cirilli

Salvatore d'Emilio

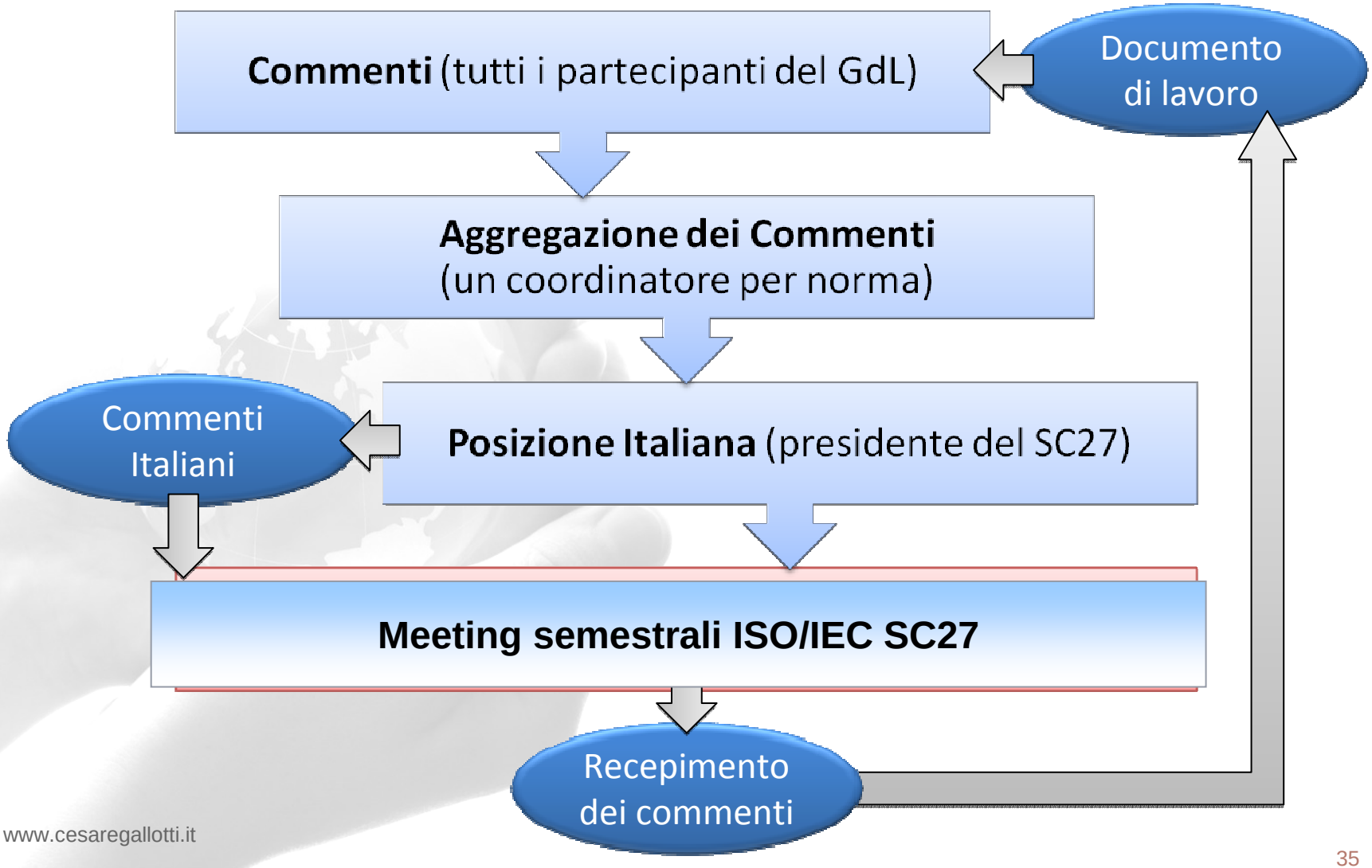
Nunzio Gagliardi

Cesare Gallotti

Gianpietro Trovesi

Aziende

Attività del GdL



Grazie!

- Cesare Gallotti
  cesaregallotti@cesaregallotti.it
  http://www.cesaregallotti.it
  http://blog.cesaregallotti.it
  PEC: cesaregallotti@mailcert.it

Le foto (viaggi di lavoro)

- Slide 2: 2006-02-02-Aereo-Zagabria
- Slide 7: 20100903-Atyrau (Europa e Asia)
- Slide 9: 20071107-Marocco
- Slide 10: 2006-10-06-Atene
- Slide 11: 20071119-SudAfrica
- Slide 12: 2006-10-06-Atene
- Slide 15: 20070514 Brescia
- Slide 16: 20070717-Valencia
- Slide 21: 20070718-Madrid
- Slide 22: 20071211-Marrakesh
- Slide 24: 20080107-Bilbao
- Slide 25: 20090803-Vigo
- Slide 26: 20100701-Cornetto a Catania
- Slide 28: 20100118-Budapest
- Slide 29: Atyrau – Fiume Ural
- Slide 30: 20101212-Volubilis
- Slide 37: 20111109-Jacaranda a Pretoria