

 Bassilichi

1^ Forum PCI ITALIA

Milano, 7 aprile 2011

**Protezione dei dati:
Certificazione PCI DSS e ISO 27001**

Ferdinando Soldan

Direttore Compliance Aziendale

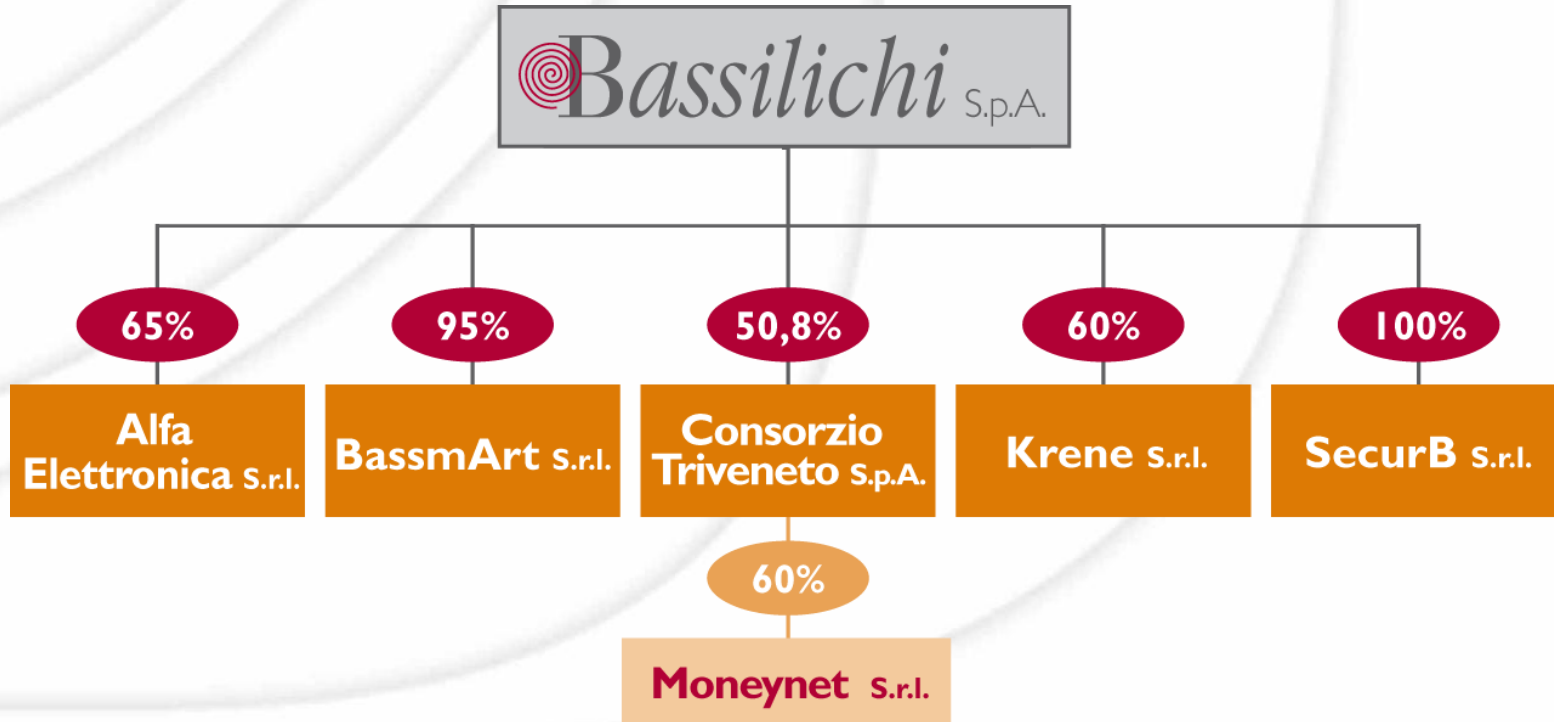
Bassilichi S.p.A.



Operatore a livello nazionale attivo nell'ambito
del **Business Process Outsourcing** (BPO).

Si posiziona quale partner strategico
di Banche, Aziende ed Enti della Pubblica Amministrazione
con un'offerta che copre quattro aree:
Monetica, Back Office, Sicurezza e Facility Management.

Le aziende controllate



Alfa Elettronica S.r.l.

Progettazione e produzione sportelli self service

BassmArt S.r.l.

Attività di biglietteria elettronica e merchandising

Consorzio Triveneto S.p.A.

Servizi nell'ambito della Monetica e del Corporate Banking

Krene S.r.l.

Attività di sviluppo software e sistemi informativi

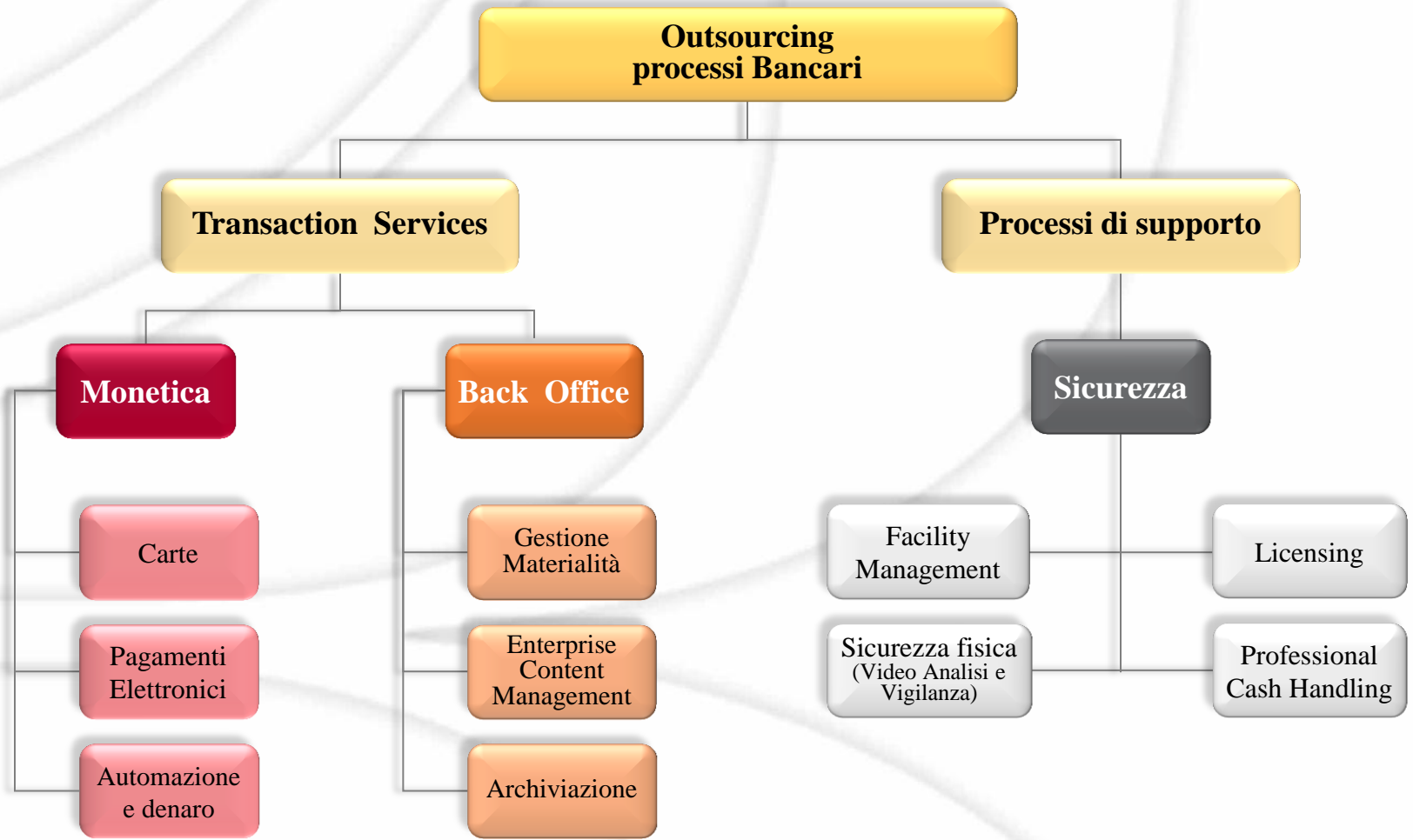
Moneynet S.r.l.

Servizi nell'ambito della Monetica

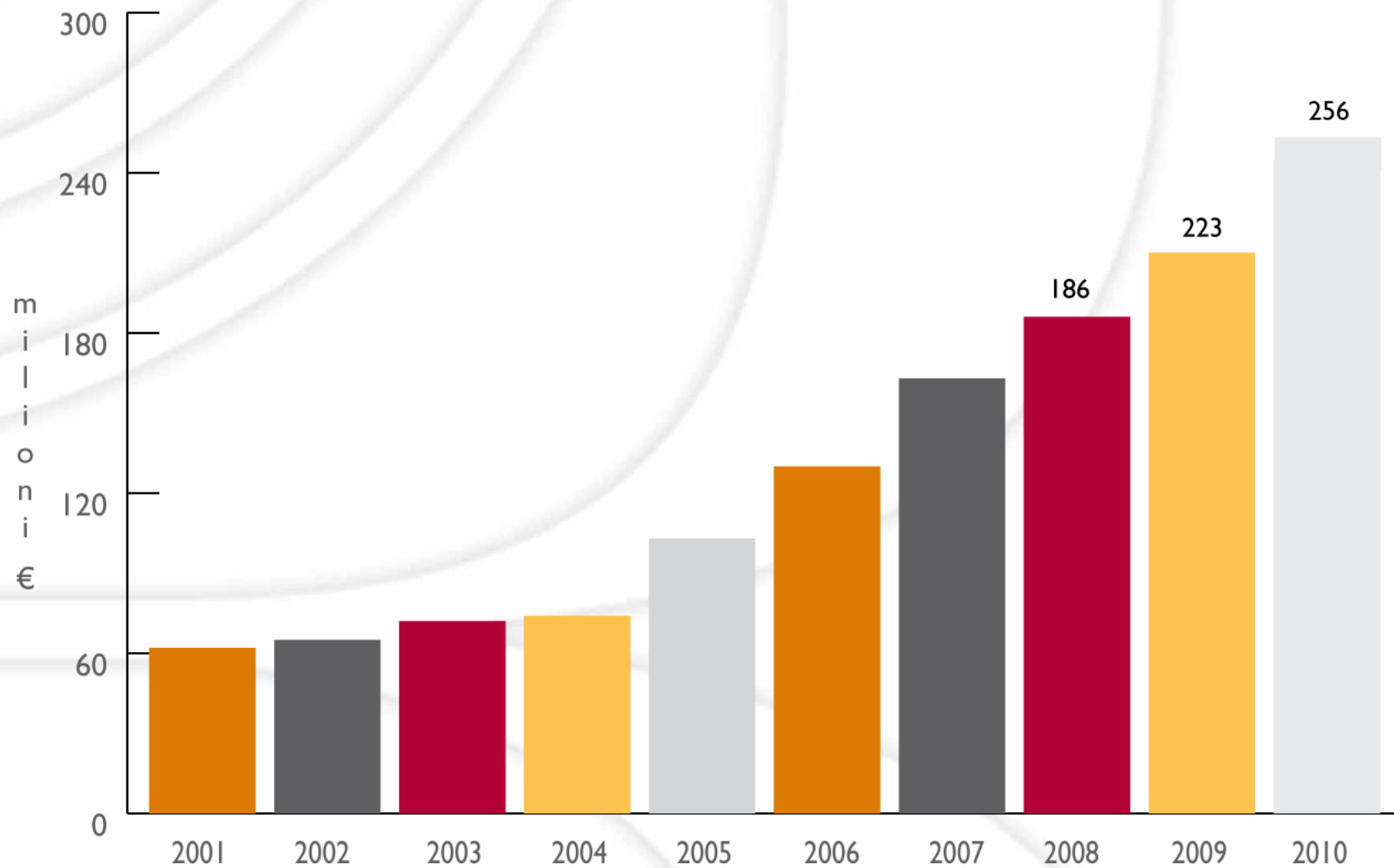
SecurB S.r.l.

Servizi nell'ambito della Sicurezza

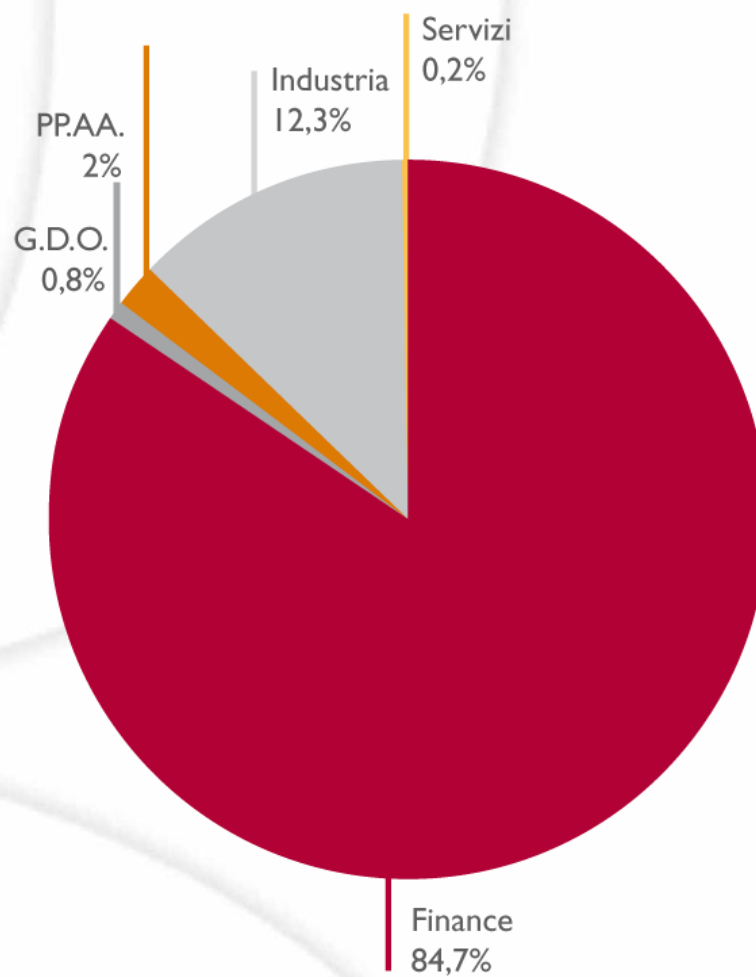
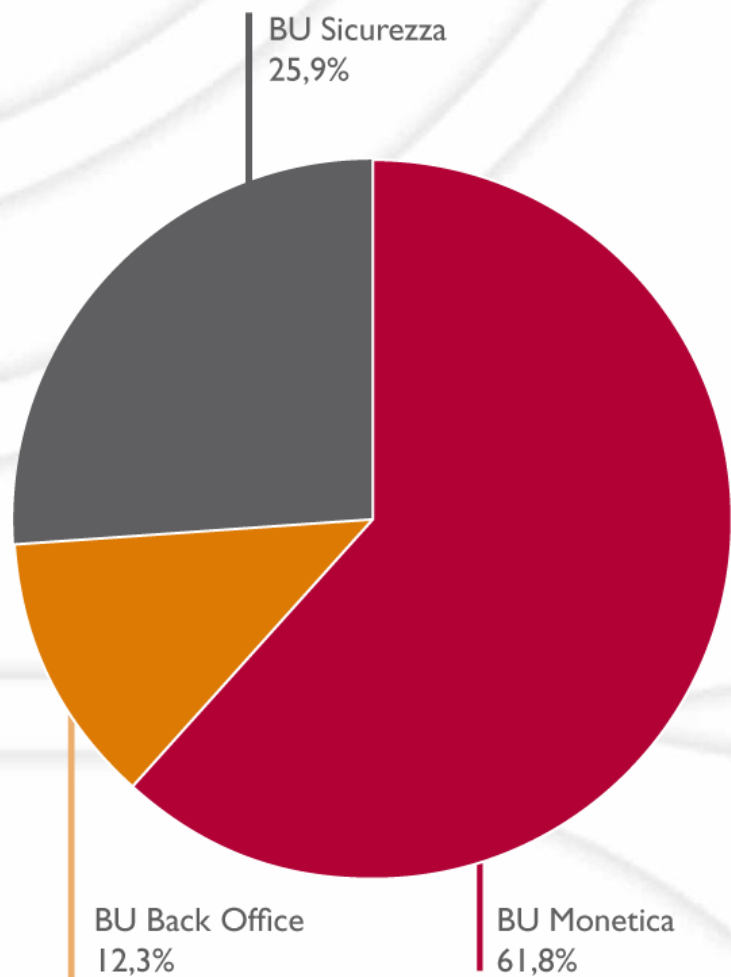
Il modello di business



Il fatturato



Analisi dei ricavi



Basilichi sul territorio





Il Consorzio Triveneto S.p.A. nasce nel 1990
per progettare, sviluppare, promuovere e gestire servizi
innovativi con gli strumenti offerti dall'evoluzione tecnologica
nell'ambito di qualsiasi **sistema di pagamento.**

A gennaio 2009 entra a far parte del gruppo Basilichi per
consolidare l'offerta dei servizi di Monetica.

Alcuni numeri



Oggi: oltre 150 persone su tre ambiti di servizio:

- Monetica (Pos, e-Commerce)
- Corporate e Internet Banking
- Servizi innovativi di pagamento

FATTURATO 2010: 30 Milioni di € (circa il 70% servizio POS)

INVESTIMENTI 2010: 5,5 Milioni di € (70% attrezzature Ind. e Comm.)

Servizio Pos

- Parco POS (31-12-2010): 207.000
- Transazioni di acquisto: 278 milioni
- Importo acquisti: 20.000 milioni di €

Servizio e-Commerce

- Totale transazioni di acquisto: 5,4 milioni

Corporate Banking Interbancario

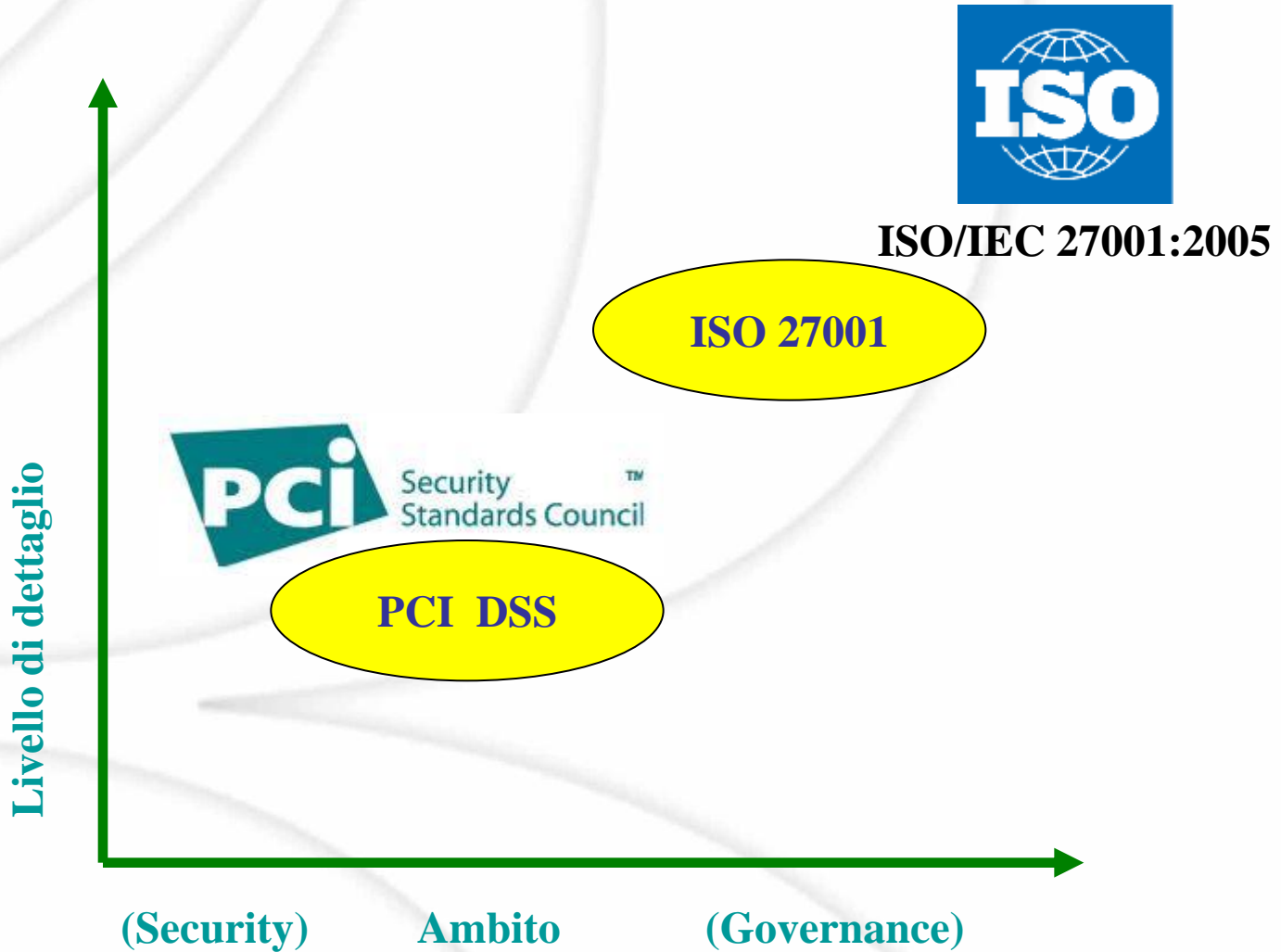
- Totale Aziende utenti: 125.000 unità
- Totale disposizioni: 24 milioni
- Valore movimentato: 80 miliardi di euro





- ✓ Il Consorzio Triveneto è certificato PCI DSS dal gennaio 2007
- ✓ Nel 2010, anche a seguito del nuovo profilo aziendale, maggiormente rivolto al mercato, viene deciso l'avvio del processo di **certificazione ISO 9001 ed ISO 27001**
- ✓ L'obiettivo era puntare sul completamento di un sistema di gestione della qualità attivo dal 2005 (non portato in certificazione) e soprattutto **valorizzare il sistema di sicurezza** realizzato per la certificazione **PCI DSS**

Confronto tra gli standard



Confronto tra gli standard



A differenza del PCI DSS, lo standard ISO 27001 è più flessibile in termini di ambito, obiettivi, controlli e conformità

- la 27001 si applica ad una generica organizzazione
- il PCI-DSS si applica ai trattamenti di cardholder data

I controlli PCI-DSS sono obbligatori, quelli 27001 sono basati sul risk appetite dell'azienda.

27001 aggiunge al PCI-DSS i requisiti di un sistema di gestione: analisi dei rischi, piano di audit, indicatori di efficacia,

Confronto tra gli standard



PCI DSS

- ✓ Focus sulle criticità di chi gestisce transizioni con carte di pagamento, indica direttamente le contromisure minime necessarie
- ✓ Definisce ed imposta il livello di sicurezza richiesto
- ✓ Dominio definito sulla base dei requisiti dello standard
- ✓ Frequente aggiornamento (inizialmente ogni 2 anni, dal 2010 ogni 3)
- ✓ Verifica esterna annuale, considera tutti i requisiti

ISO 27001

- ✓ Focus sul Sistema di Gestione, basato sul ciclo di Deming
- ✓ Lascia all'organizzazione la definizione del livello di rischio "accettabile"
- ✓ Dominio definito dall'organizzazione
- ✓ Aggiornamento medio periodo (l'ISO 27001 è datata 2005)
- ✓ Verifica esterna annuale

Confronto tra gli standard



Un altro confronto di caratteristiche:

	PCI DSS	ISO27001
Implementazione dei controlli	Obbligatoria	Basata su analisi del rischio
Granularità	Alta	Bassa
Flessibilità	Bassa	Alta
Sistema di Gestione	Relativo	Essenziale



Mettere assieme PCI-DSS e 27001



Tre possibilità teoriche:

- 1) Avviare un progetto comune per 27001 e PCI-DSS
- 2) Partire da una situazione (certificata?) ISO 27001 e poi raggiungere la compliance PCI-DSS
- 3) Viceversa, partire da una compliance PCI-DSS e raggiungere la certificazione 27001

La 1) porta maggior efficacia ed efficienza nell'implementazione

La 2) è il percorso più logico, perché aggiunge un livello di dettaglio ai requisiti 27001. Il sistema di contesto (SGSI) è sicuramente valido e mantenuto, a seconda del livello di applicazione dei controlli 27001/PCI-equivalenti, il gap di implementazione sarà più o meno elevato

La 3) si tratta di norma-lizzare secondo la 27001 l'esistente



Progetto avviato ad inizio febbraio 2010 con una Gap Analysis rispetto ai requisiti ISO 27001

I risultati, in linea con le attese e con le differenze tra gli standard, hanno evidenziato:

- Controlli in essere adeguati
- Metodologia di analisi del rischio da rivedere
- Un sistema di gestione integrato da completare con i requisiti comuni ai due sistemi di gestione (SGSI e SGQ)
- Necessità di diffusione della consapevolezza sui requisiti dalla norma



Necessità di implementare e consolidare alcune misure organizzative per passare da un framework di controlli (PCI-DSS) ad un sistema di gestione per la sicurezza.

Il PCI-DSS ha costituito l'input per la definizione dei controlli ma ha dettato solo parzialmente gli elementi per la predisposizione di un sistema di gestione (SGSI)



La definizione di un **Sistema di Gestione Integrato** ha compreso in particolare i processi di audit, documentazione, formazione, HR, approvvigionamenti,
(difficile separare attività per SGQ da SGSI)

- E' stato attivato un Audit specifico sul sistema di gestione (oltre che sui controlli, già attivo)
- Sono stati redatti 3 nuovi documenti su circa 40 esistenti che costituiscono il sistema documentale per la sicurezza (policy, procedure, ...).

Altri temi rilevanti per la security sono stati:

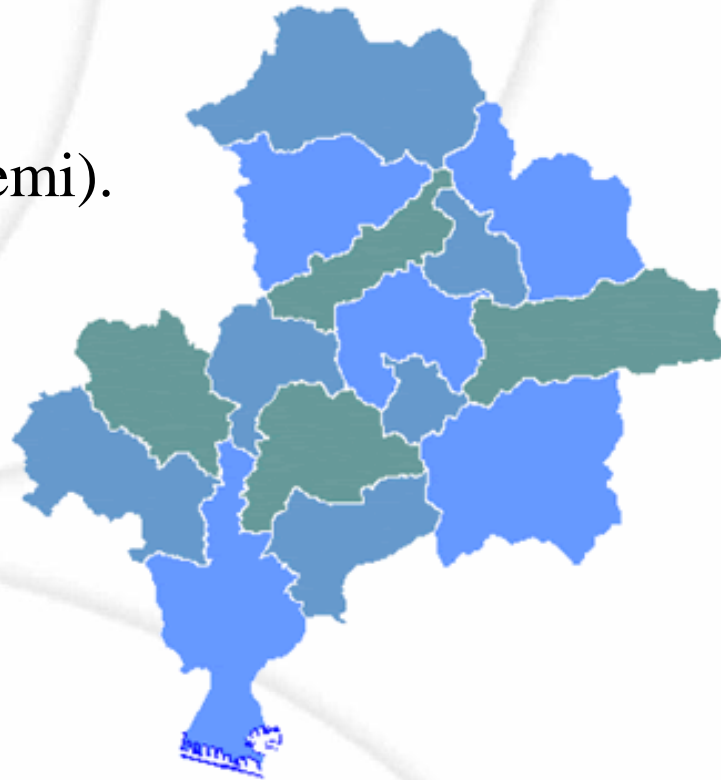
- **Ambito**
- **Analisi del rischio**
- **Controlli**
- **Indicatori**



L'ambito PCI-DSS è definito dallo standard, per la 27001 abbiamo scelto invece un ambito comprendente tutti i servizi erogati alla clientela (*).

Questo ha implicato una estensione dell'ambito di circa il 40% (persone, sistemi).

(*) L'ambito per la 9001 è più confinabile, quello per la 27001 è più pervasivo

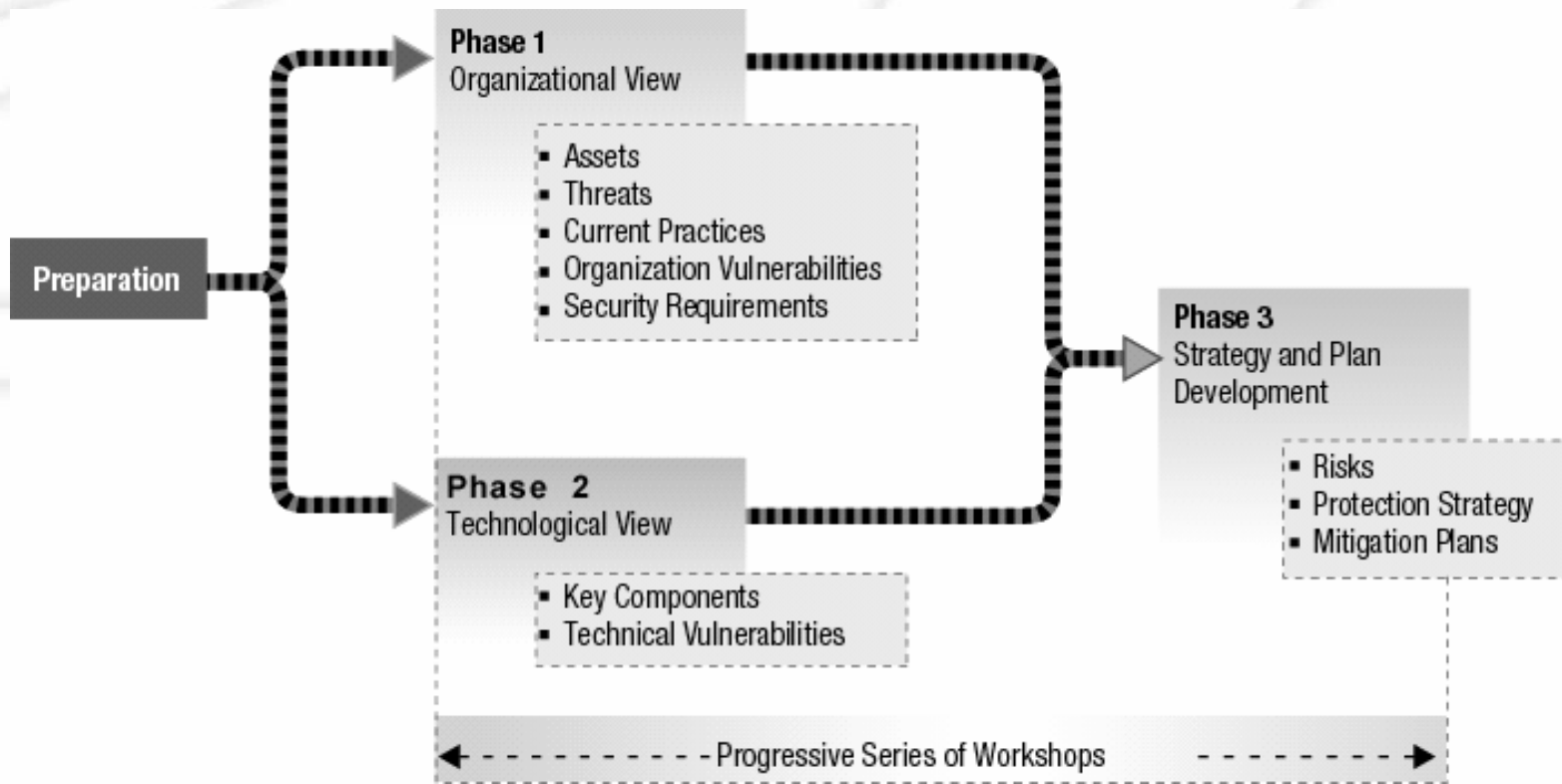


Analisi del rischio



Dal 2006 è stata introdotta in azienda la metodologia Octave (CMU-SEI) per l'Analisi del rischio.

E' stata formalizzata la metodologia in essere, descrivendo i criteri di accettazione del rischio, la selezione dei controlli, la connessione tra impatti e controlli.





La SOA comprende 131 dei 133 controlli della norma.

Normalmente il controllo 27001 è meno dettagliato e meno stringente (demandato all'organizzazione e legato al rischio) dell'analogo PCI-DSS (che conta circa 200 controlli)

Non sono state effettuate implementazioni riguardanti i controlli tecnologici.

Nella nostra implementazione, la baseline di sicurezza realizzata per gestire le reti ed i sistemi, già rivista annualmente secondo una analisi del rischio estesa anche ai sistemi non PCI, è stata riconosciuta adeguata al livello richiesto dalla 27001 per tutto il dominio, mentre il livello più stringente dei controlli PCI-DSS rimane confinato al rispettivo dominio PCI.

Indicatori



Si è proceduto ad identificare (secondo le linee guida della ISO 27004) un elenco di indicatori relativi al SGSI

La misura degli indicatori è un **elemento essenziale per il Sistema di Gestione**, non è requisito evidente per il PCI-DSS



DIFETTI DELL'ALTRO



INNALZAMENTO BARRIERE



AFFERMAZIONI ASSOLUTE



SI PARLA DI COLPA

Il progetto



Durata del progetto (*):

Circa 8 mesi (a partire dalla Gap Analysis)

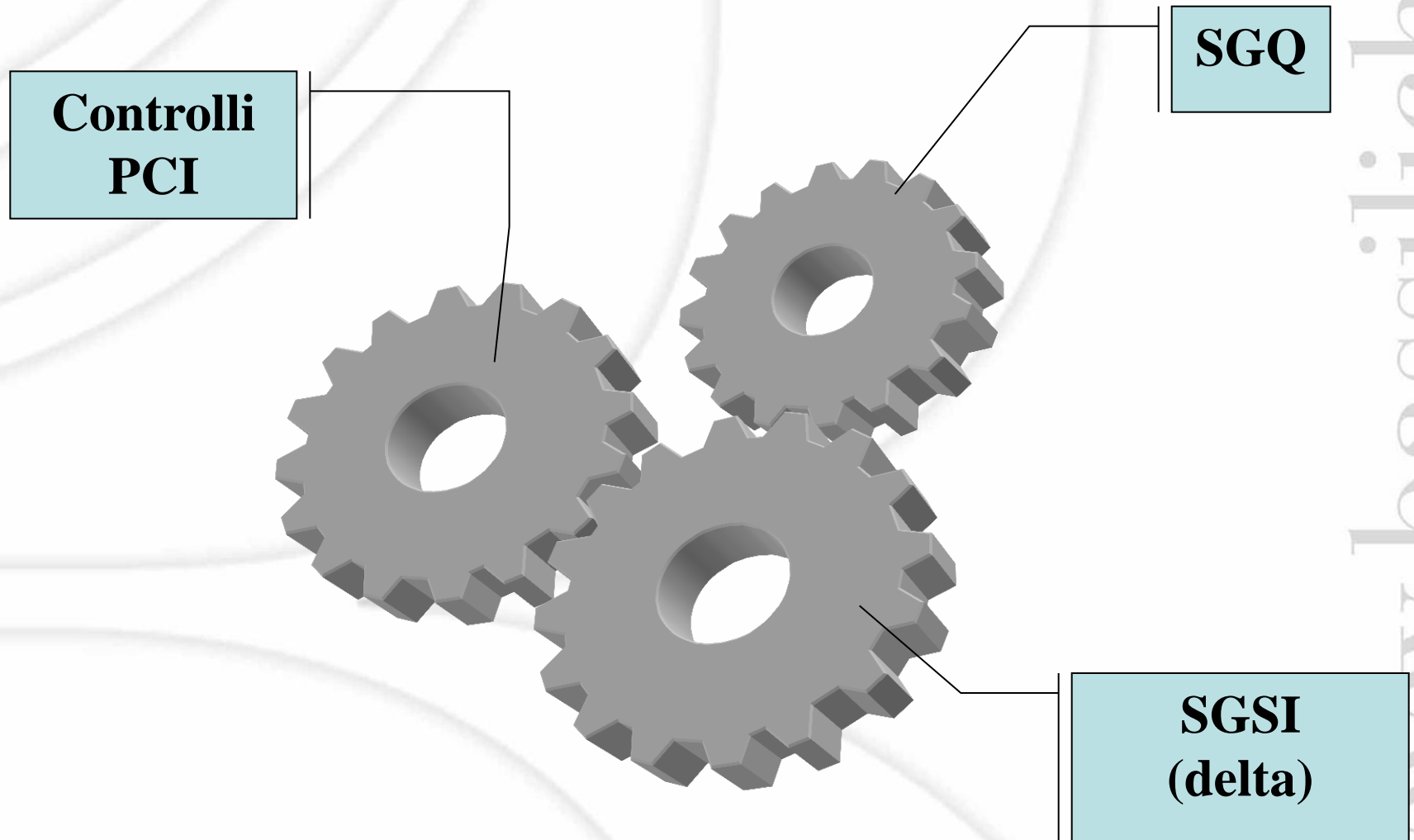
Team di 3 persone più supporto esterno

(collaborazioni per 60 gg. circa)



(*): Includere le attività per il completamento del SGQ/SGSI

Il combinato disposto ...



Il percorso ...



“Ogni *lunga marcia* comincia con un piccolo *passo*”

Il percorso che oggi ci ha portato alle certificazioni PCI e ISO 27001/9001 si è sviluppato negli anni:

- Nuova architettura di rete (2003)
- Identity management (2004)
- Prima definizione di Security Policy & Standard (2005)
- Utilizzo di OCTAVE per risk analysis (2006)
- **Certificazione PCI DSS** (gennaio 2007)
- Business Continuity Plan.... (2008)
- Formazione specialistica sulla sicurezza (da 2009)
- **Certificazione ISO 27001** (2010)



Risultati raggiunti



L'obbligo della certificazione PCI ha consentito di superare una prima soglia d'ingresso, avviando successivamente un processo virtuoso che ha potuto avvalersi dei risultati già raggiunti.

→ Compliance PCI DSS

→ Certificazione ISO 27001

→ **Modello di organizzazione gestione e controllo**

(in particolare per la parte speciale relativa ai **reati informatici**)

Il processo di compliance si sviluppa secondo una spirale rovesciata in cui allontanandosi dal dettaglio l'ambito viene progressivamente allargato spostandosi verso la Governance



Grazie per l'attenzione!



Domande?

ferdinando.soldan@bassilichi.it