ORACLE

Sicurezza e Continuità Operativa
per la PA e la Sanità: Roadshow

- SICUREZZA
- CONTINUITÀ OPERATIVA

Il punto di vista della conformità e della certificazione volontaria

ROMA - FORUM PA - 18 MAGGIO 2012

I Sistemi di Gestione e le norme ISO: un percorso virtuoso

Da giovane programmatore mi dissero che esistevano tre modi per fare le cose:

- Bene
- Male
- e … come vuole il cliente

Con il tempo ho scoperto che non era vero perché le cose non si fanno …. si gestiscono.

I Sistemi di Gestione e le norme ISO: un percorso virtuoso

Il concetto è che dobbiamo imparare a gestire quello che sappiamo fare. Proviamo un parallelo:

"L'intelligenza finanziaria non ha tanto a che fare con quanto guadagni ma con quanto riesci a mettere via" e ancora: *"Le persone (realmente) ricche non raccolgono le loro maggiori entrate dal loro lavoro ma dalla resa dei loro investimenti"*

In altre parole non dal fare ricaviamo i maggiori profitti ma dal gestire quello che sappiamo fare. Potremmo dire che la sola **competenza del fare** non basta.

I Sistemi di Gestione e le norme ISO: un percorso virtuoso

Il concetto è che dobbiamo avere un buon sistema per gestire al meglio quello che sappiamo fare.

Questo ci permetterà di ricavare i maggiori *profitti* dalla nostra attività, qualsiasi essa sia.

Ma come fare per avere un buon sistema di gestione?

Panorama normativo:

Information Security

I Sistemi di Gestione e le norme ISO: un percorso virtuoso

I Sistemi di Gestione fanno riferimento in primis all'esperienza condivisa e poi alle norme (UNI, CEN, ISO) che nascono da lunghi e condivisi iter e che sono sottoposte a costante controllo e miglioramento.

Norme che entrano a far parte di un sistema di accreditamento e di certificazione che fornisce garanzia al mercato, nella sua più ampia accezione.

I Sistemi di Gestione abilitatori delle nostre attività

- Il concetto base – che risiede nelle volontarietà dei sistemi ISO – è la volontà (= necessità proattiva) di rispondere ad urgenze non cogenti, non dovute solo a leggi, ma alle esigenze / aspettative del cittadino (paziente) acquisendo consapevolezza (awareness) della suddetta volontà (retroazione virtuosa) di dare risposte nuove (competitività) alle parti interessate.
- I Sistemi di Gestione intesi e utilizzati come abilitatori di questa volontà e come driver di opportunità capaci di guidare, indirizzare le sempre nuove (e non sempre prevedibili) necessità di governance.

L’informazione

“L’informazione è una risorsa che, al pari di altri beni che costituiscono il patrimonio di un’azienda, rappresenta un valore per l’organizzazione e necessita pertanto di essere adeguatamente protetto”

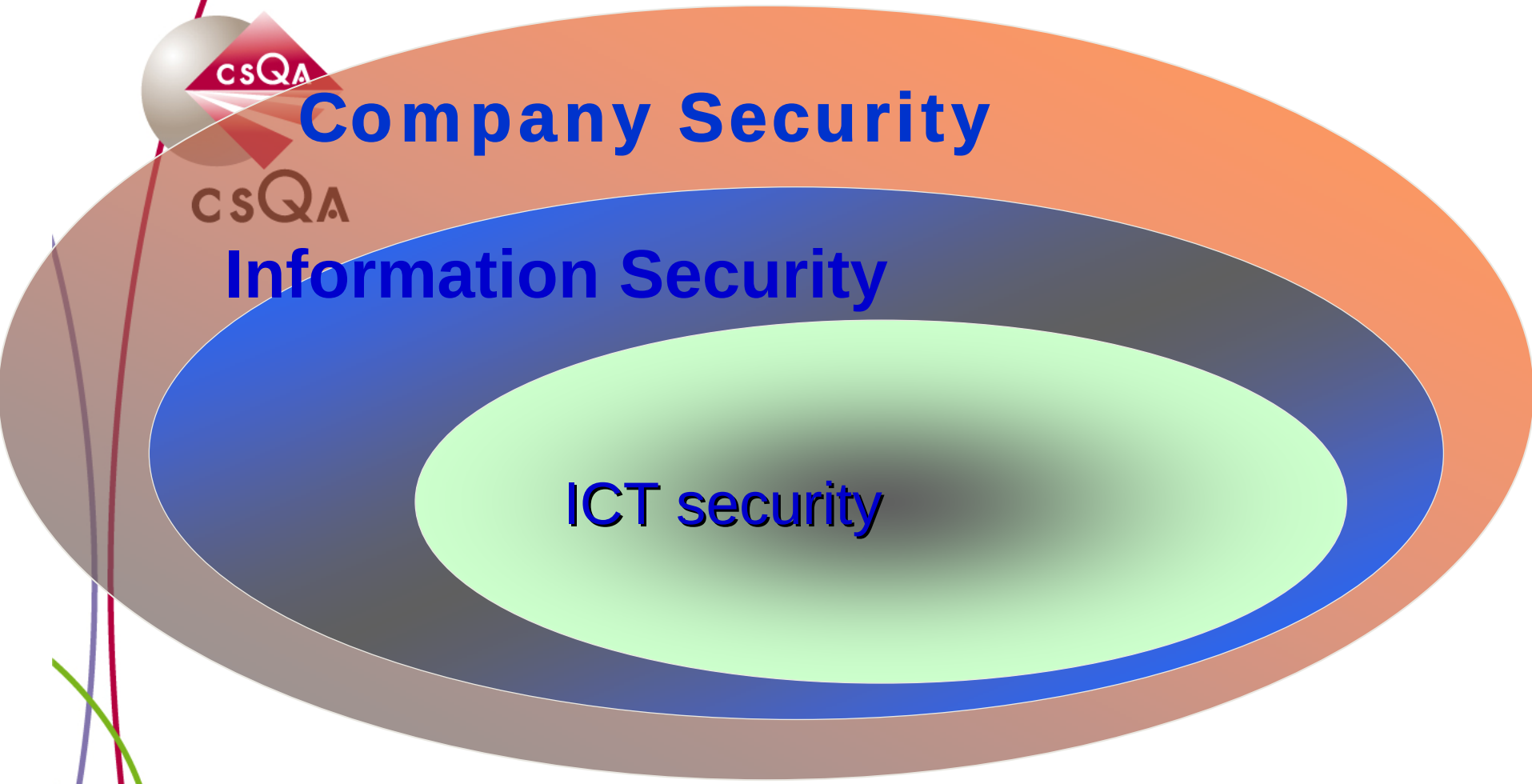
ISO/IEC 27002:2005

L’informazione può esistere in tante forme

- *Stampate o scritte su supporto cartaceo*
- *Memorizzate elettronicamente*
- *Trasmesse via posta o mezzi elettronici*
- *Registrate su video*
- *Verbali – Trasmesse nell’ambito di conversazioni*
- *… …*

“ … … Qualunque forma assumano le informazioni, e qualunque siano i mezzi con cui vengono condivise o memorizzate, vanno sempre adeguatamente protette.”

ISO/IEC 27002:2005



L'ICT Security si inquadra nel contesto più ampio dell'Information Security, questa a sua volta va considerata nell'ambito più esteso di Company Security.

Facciamoci alcune domande

Come deve essere realmente affrontato il problema?

Posto che qualcosa devo fare per tutelarmi:

cosa faccio?
come lo faccio?

Lo devo fare e devo avere un piano?

come posso avere una lista esaustiva dei controlli da applicare?

esiste un metodo che fornisce buoni livelli di sicurezza e i risultati attesi?

come faccio a fornire all'esterno evidenza incontroversibile della mia diligenza?

I Sistemi di Gestione declinati per la Sicurezza delle informazioni e la continuità operativa

I vantaggi delle migliori pratiche internazionali riportati nel contesto reale della Pubblica Amministrazione e Sanità Italiana

In particolare ci riferiamo oggi alla norma:

UNI CEI ISO/IEC 27001:2006

Information tecnnology – Security techniques – Information security management systems – Requirements

che rappresenta il riferimento assoluto per chi vuole gestire il problema della sicurezza dei dati (digitali e non).

La norma ISO/IEC 27001 definisce i requisiti per un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) ed è progettata per garantire la selezione di controlli di sicurezza adeguati e proporzionati.

Set della documentazione SGSI

- Politica della sicurezza delle informazioni;
- Dichiarazione del campo di applicazione;
- dichiarazione di applicabilità (SOA);
- Inventario delle risorse informative e di sistema da proteggere;
- Valutazione del rischio;
- Procedure e standard applicabili;
- Contratti (SLA, accordi sull'uso accettabile, ecc..)

Guidati dalla documentazione di "processo"

Processi aziendali

Eventi

- Incidenti alla sicurezza;
- Debolezze presunte;
- Malfunzionamenti.

- Osservazioni degli audit;
- Risultati di test;
- Risultati di controlli a campione (*spot-check*)

Evidenze

Registrazione e analisi

Verbale(i) all'interno di un forum

Riesame ed aggiornamento del SGSI

Per rispondere alle recenti esigenze

- Le ultime modifiche al **Codice dell'Amministrazione Digitale** apportate dal D.Lgs. 235/2010 hanno introdotto importanti indicazioni in tema di continuità del servizio e di reingegnerizzazione dei processi. In particolare, l'articolo 50-bis sancisce che **le Pubbliche Amministrazioni devono predisporre un piano di Disaster Recovery e di Business Continuity** a salvaguardia dei servizi erogati a cittadini e aziende.

Ma la continuità dei servizi è **più un'opportunità che un obbligo di legge**

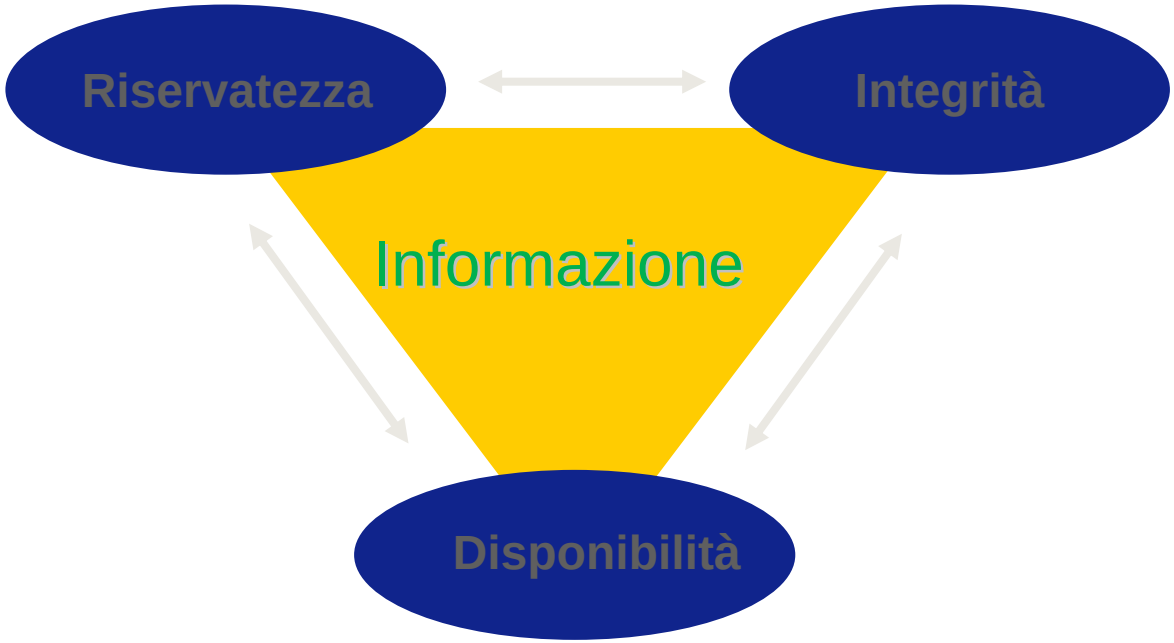
- L'opportunità di dotarsi di strumenti di gestione dei rischi risulta particolarmente rilevante nel caso della Pubblica Amministrazione, per l'entità della ricaduta sulle parti interessate, che in questo caso coincide con il tessuto sociale del Paese: in tal caso la gestione virtuosa delle attività comporta il miglioramento della "qualità della vita sociale".

Gli Enti devono imparare ad affrontare queste tematiche con **nuovi strumenti e metodologie**.

- L'obiettivo è quello di partire dagli adempimenti richiesti dal Codice per delineare un percorso coerente e strutturato verso un **Sistema di Gestione della Sicurezza delle Informazioni** (SGSI) **a norma ISO 27001** all'interno della propria organizzazione, in grado di armonizzare ed integrare tutti gli adempimenti legati alla **sicurezza delle informazioni.**

Un breve approfondimento …

La sicurezza delle informazioni significa la salvaguardia di



Obiettivi della ISO 27001

Riservatezza

La proprietà in virtù della quale le informazioni non sono rese disponibili o divulgate a individui, entità o processi che non sono autorizzati (da ISO/IEC 13335-1:2004).

Integrità

La proprietà di salvaguardia dell'accuratezza e della completezza degli asset (da ISO/IEC 13335-1:2004).

Disponibilità

La proprietà in virtù della quale le informazioni sono rese accessibili e utilizzabili su richiesta di una entità autorizzata (da ISO/IEC 13335-1:2004).

E ancora, da questi declinabili, altri obiettivi :

Autenticità

La proprietà in virtù della quale viene garantito che l'identità di un soggetto o di una risorsa sia quella dichiarata [dal soggetto o dalla risorsa]. L'autenticità si applica a entità quali utenti, processi, sistemi e informazioni (da ISO/IEC 13335-1:2004).

Non ripudio

La capacità di provare che un'azione o un evento ha avuto luogo, in modo tale che non si possa successivamente affermare che tale azione non sia avvenuta (da ISO/IEC 13335-1:2004).

Accountability

La proprietà che assicura che le azioni effettuate da un entità possano essere tracciate e fatte risalire all'entità (da ISO/IEC 13335-1:2004).

Un po' di storia

1990 DTI (Department of Trade and Industry) britannico istituisce un gruppo di lavoro per linee guida gestione sicurezza del sistema informativo

1993 Il gdl produce raccolta di "best practice" per gestione della sicurezza del S.I.

1995 British Standard Institution pubblica lo standard BS 7799-1 "Code of Practice for ISMS"

1998 BSI pubblica BS 7799-2 "Specification for Information Security Management Systems"

1999 BSI pubblica un aggiornamento dei due standard

2000 il Comitato ISO pubblica la ISO/IEC 17799:2000 (dallo standard BS 7799-1)

2002 BSI pubblica BS 7779-2:2002 adeguandola ai Sistemi di Gestione (inserendo PDCA);

vengono emessi i principi dell'OCSE

2005 ISO pubblica revisione ISO/IEC 17799 e ISO/IEC 27001 – nasce la nuova ISO 27000 family

2006 la norma ISO/IEC 27001 viene recepita e tradotta dall'UNI e diventa UNI CEI ISO/IEC 27001:06

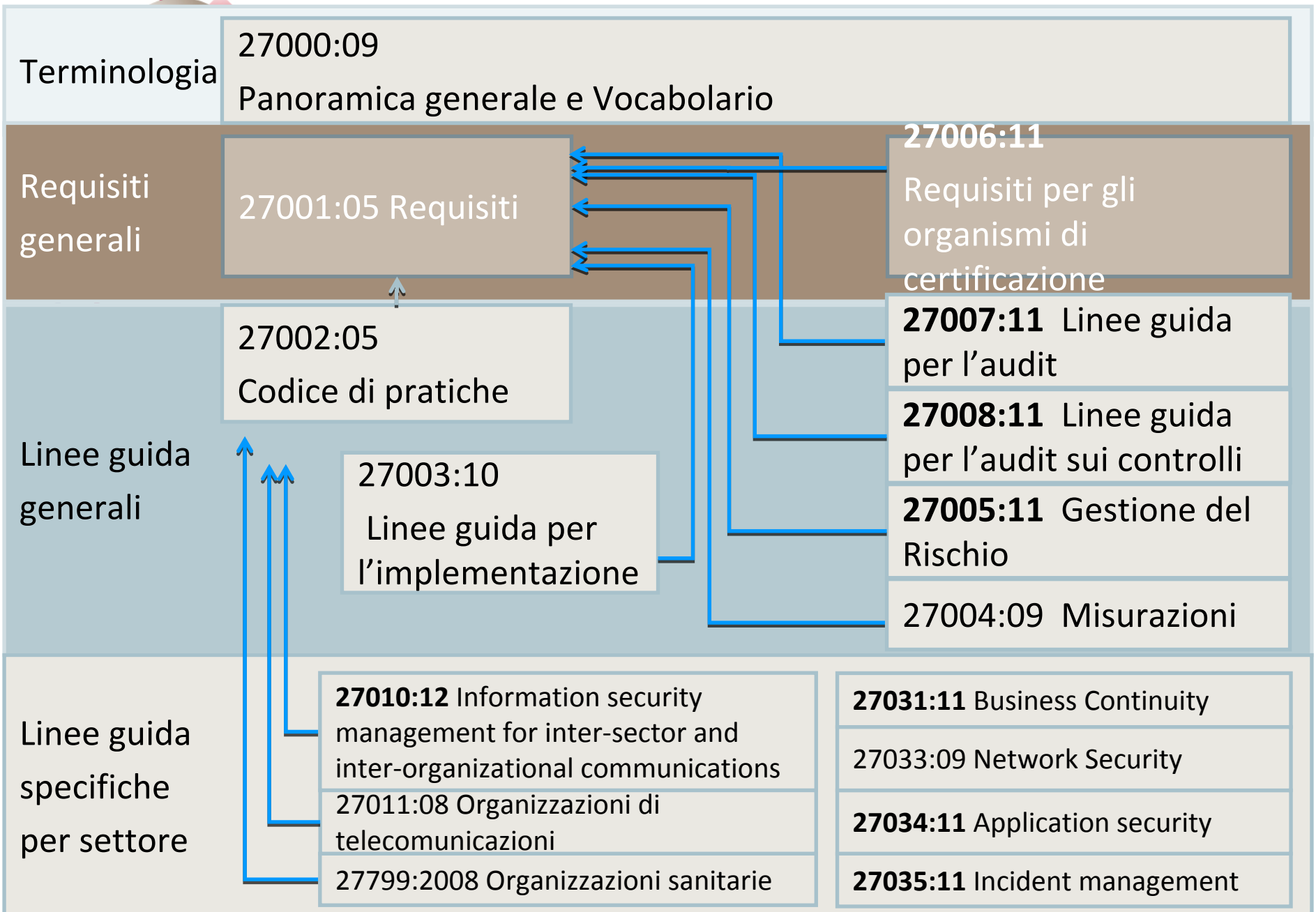
2007 la ISO/IEC 17799 viene rinominata ISO/IEC 27002; viene pubblicata la ISO/IEC 27006

2008 la ISO pubblica le norme: ISO/IEC 27005; ISO 27799 e ISO/IEC27011

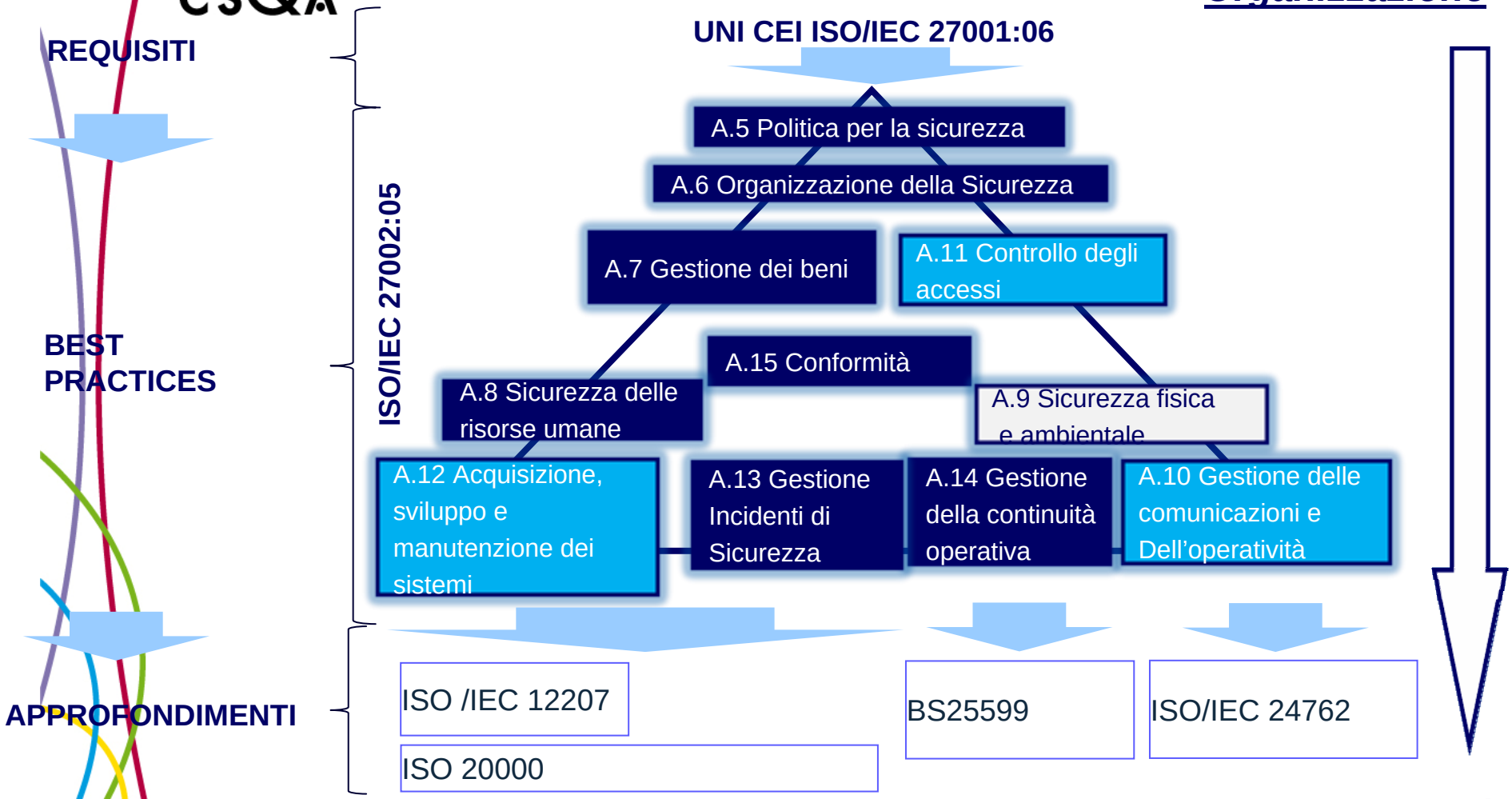
2009 la ISO pubblica la norma ISO 27000 "Overview and vocabulary"

2010 la ISO pubblica le norme: ISO 27004 e ISO 27003 .....

Famiglia delle norme ISO/IEC 27k



Dall'organizzazione della gestione all'operatività



Dall'organizzazione della gestione all'operatività … approfondimenti

- ISO/IEC 20000-1 "Information tecnology – Service management - Specification"
- ISO/IEC 20000-2 "Information tecnology – Service management – Code of practice"
- **BS 25999-1:2006 "Business continuity management. Code of practice"**
- **BS 25999–2 :2007"Specification for business continuity management**"
- ISO/IEC 24762"Information tecnology – Security tecniques – Guidelines for information and communication tecnology disaster recovery services"
- ISO/IEC 12207 "Information tecnology – Software life cycle processes"

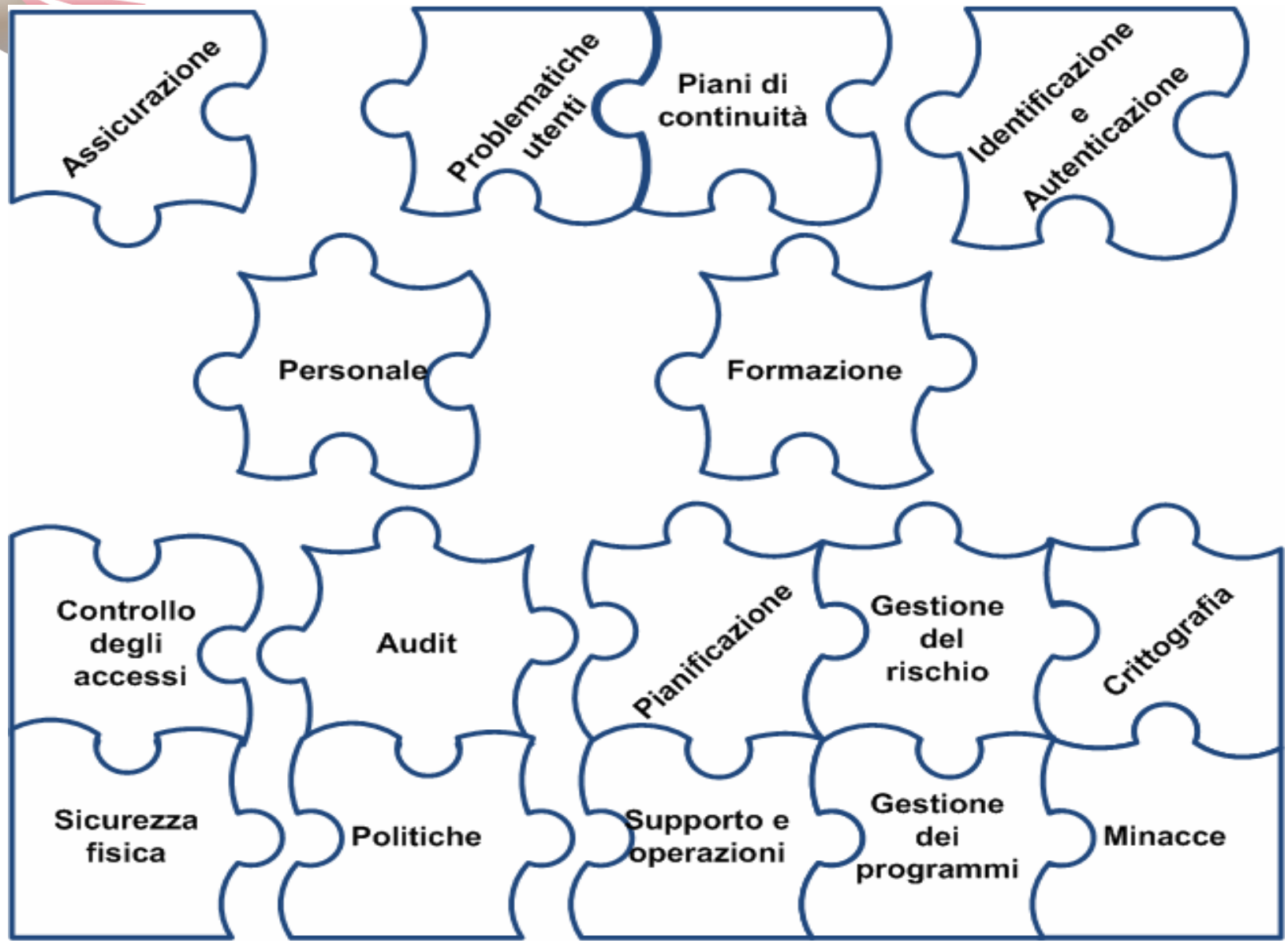
ISO 27799:2008 come applicazione specifica per la Sanità

Progettare e Gestire la Sicurezza delle Informazioni vuol dire:

Mettere in atto tutte le iniziative tecnologiche, organizzative, normative e procedurali necessarie a:

- Conoscere i rischi
- Operare per limitarli
- Essere sempre pronti a rispondere ai problemi, sia quelli previsti che quelli imprevisti

Coniugando tutti gli aspetti …



Tra cui gli aspetti cogenti

- Sono molte le norme, decreti, regolamenti, direttive UE, raccomandazioni inerenti la sicurezza delle informazioni
- L'organizzazione deve operare una attenta ricerca al fine di individuare tutti i requisiti cogenti e derivanti da regolamenti interni o con terze parti
- Il rispetto dei requisiti cogenti è un "pre-requisito" per la certificazione
- ….

Chi siamo

www.csqa.it

CSQA Certificazione è un organismo di certificazione indipendente italiano nato nel 1990.

Si occupa con professionalità e competenza di Qualità, Sostenibilità, Sicurezza, rivolgendo un'attenzione particolare alle tematiche legate alla Sicurezza delle informazioni e all'erogazione dei servizi ICT, allo scopo di fornire supporto e formazione qualificati in questo ambito in continua evoluzione.

CSQA è **accreditato Accredia** per la norma ISO 27001 e per la norma ISO 9001 per i settori legati alla tecnologia dell'informazione.

I nostri servizi: CERTIFICAZIONE

ISO/IEC 9001
Sistema di Gestione per la Qualità

ISO/IEC 27001
Sistema di Gestione della Sicurezza delle Informazioni

ISO/IEC 20000
Service Management System

UNI 11200
Servizi di call center

UNI 11068
Centrali di telesorveglianza

BS25599
Piano di Business Continuity

Il catalogo corsi completo è disponibile sul sito www.csqa.it

I nostri servizi: FORMAZIONE

Nel nostro catalogo proponiamo i seguenti corsi accreditati:

ISO/IEC 20000 Auditor con Certificazione itSMSF - Corso su richiesta

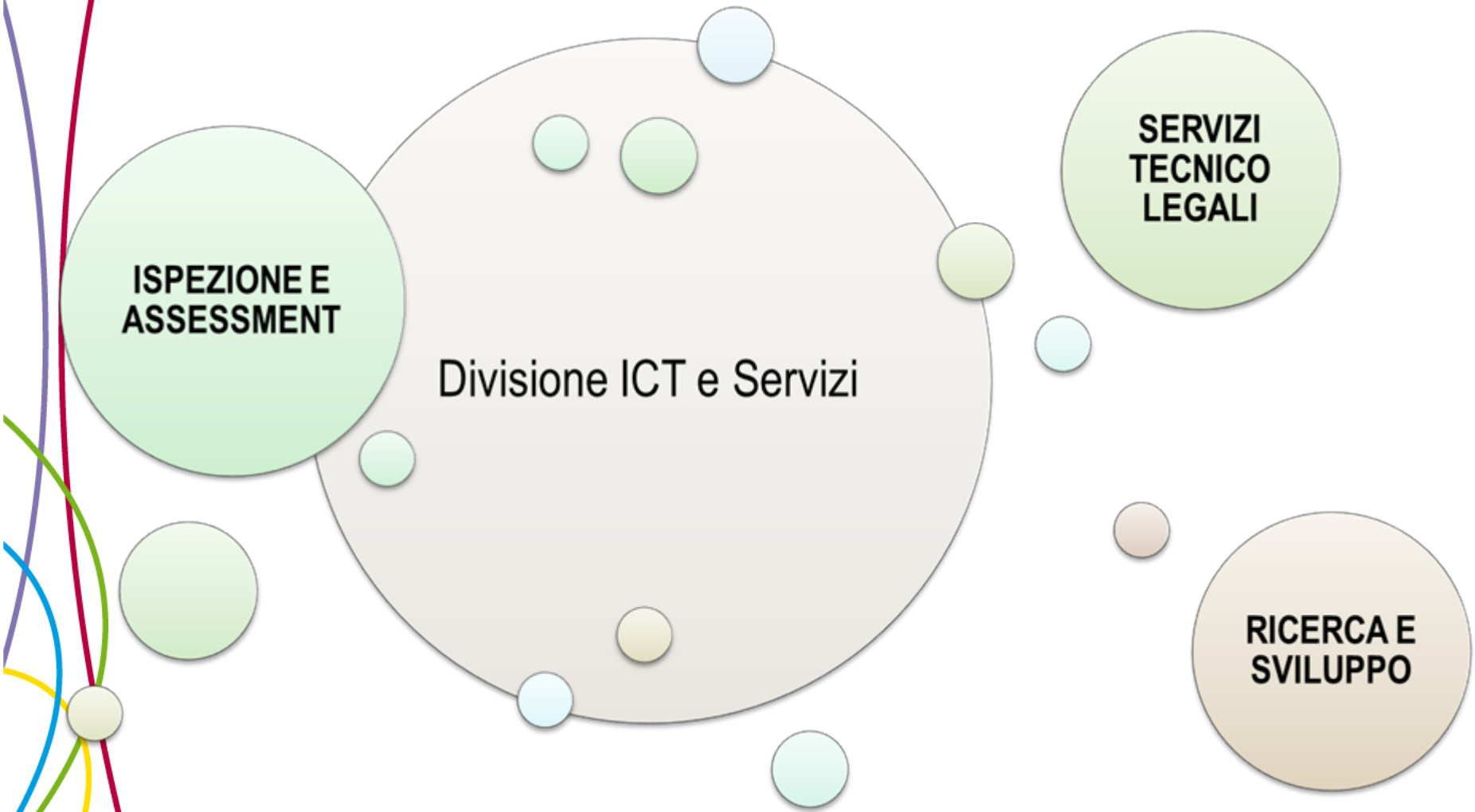
CobiT® Foundation - Corso su richiesta

ITIL® v3 Foundation con qualifica APMG/EXIN

Valutatori di Sistemi di Gestione per la Sicurezza delle Informazioni UNI CEI ISO/IEC 27001:2006 **Settore Sanitario** - Corso riconosciuto AICQ SICEV.

Valutatori di Sistemi di Gestione per la Sicurezza delle Informazioni UNI CEI ISO/IEC 27001:2006 - Corso riconosciuto AICQ SICEV.

Altri servizi

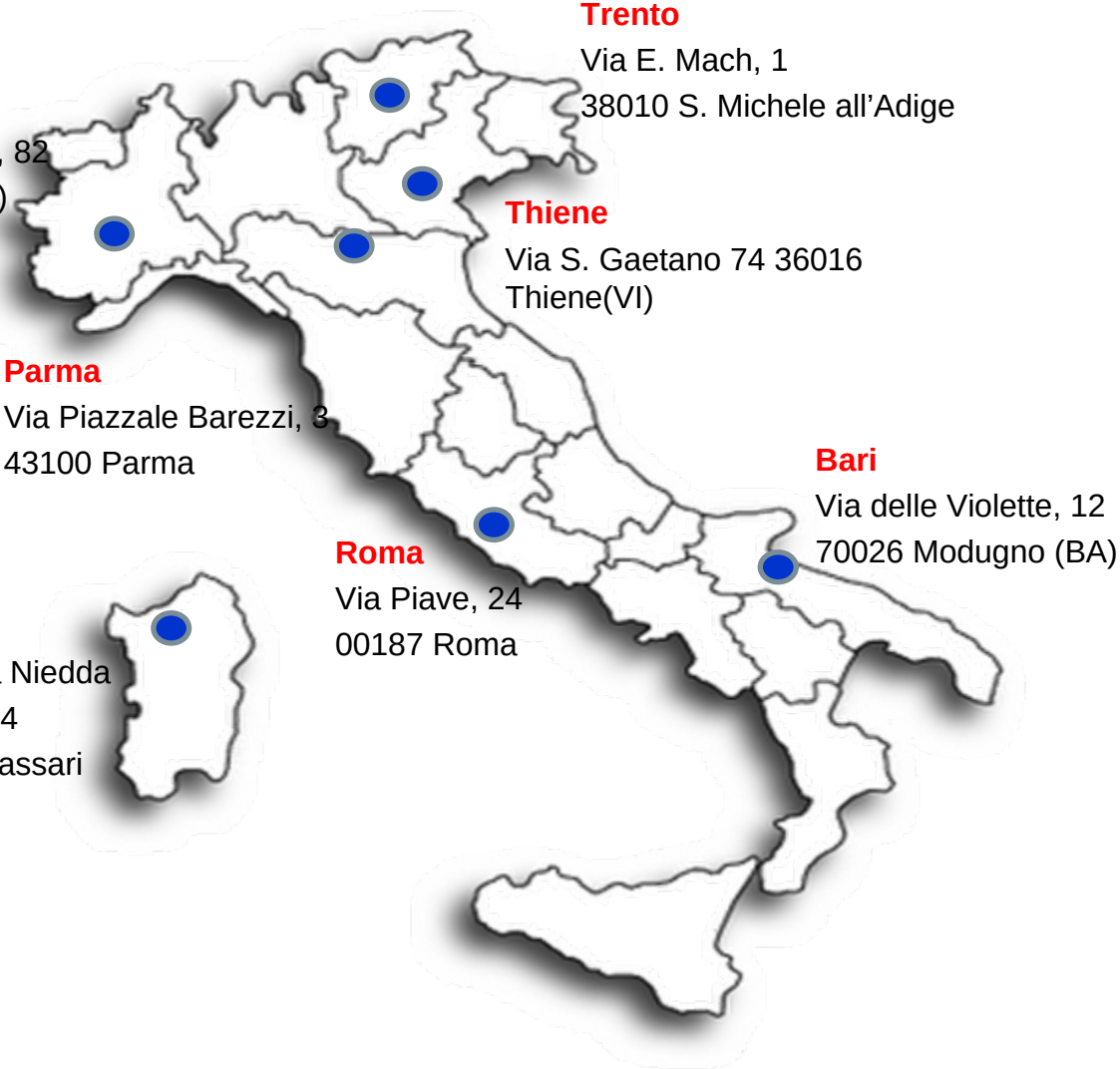


Le nostre competenze

CSQA ha un team di valutatori con esperienza e referenze, qualificati in:

- **Lead Auditor ISO 9001** - Settori EA 33 (Tecnologia dell'informazione) e 35 (Servizi professionali d'impresa)
- **Lead Auditor ISO/IEC 27001** - Registro AICQ SICEV
- **ITIL V3 Foundation** - Registro Exin
- **Lead Auditor ISO/IEC 20000** ItSMF
- **Mistery Auditor**
- CISA© - Certified Information Systems Auditor (ISACA)
- CRISC© - Certified Risk & Information Systems Control (ISACA)
- CCNA© - Cisco Certified Network Associate

Le nostre sedi



Trento
Via E. Mach, 1
38010 S. Michele all'Adige

Cuneo
Piazza C.A. Grosso, 82
12033 Moretta (CN)

Thiene
Via S. Gaetano 74 36016
Thiene(VI)

Parma
Via Piazzale Barezzi, 3
43100 Parma

Bari
Via delle Violette, 12
70026 Modugno (BA)

Roma
Via Piave, 24
00187 Roma

Sassari
ZI Predda Niedda
Str. 24 n. 4
07100 Sassari

Buona continuazione!

Ing. Bruno Bernardi

CSQA Certificazioni Srl - Divisione ICT e Servizi

e_mail: b.bernardi@csqa.it