



Convegno Clusit

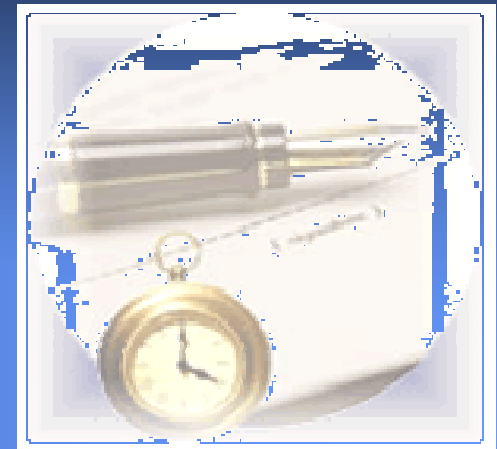
Focus sulla fornitura di Prodotti di ICT Security nei servizi di EDP outsourcing

Milano
16 Giugno 2003

All Rights Reserved

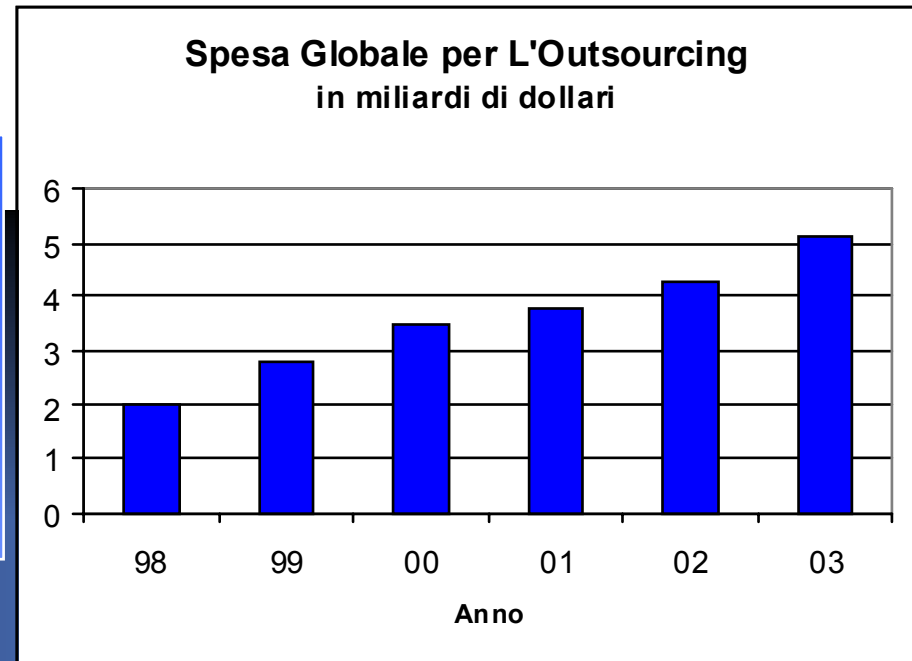
Agenda

1. *Trend di Mercato ed evoluzione nell'Outsourcing*
2. *L'approccio IBM alla sicurezza*
3. *La metodologia e le competenze IBM*



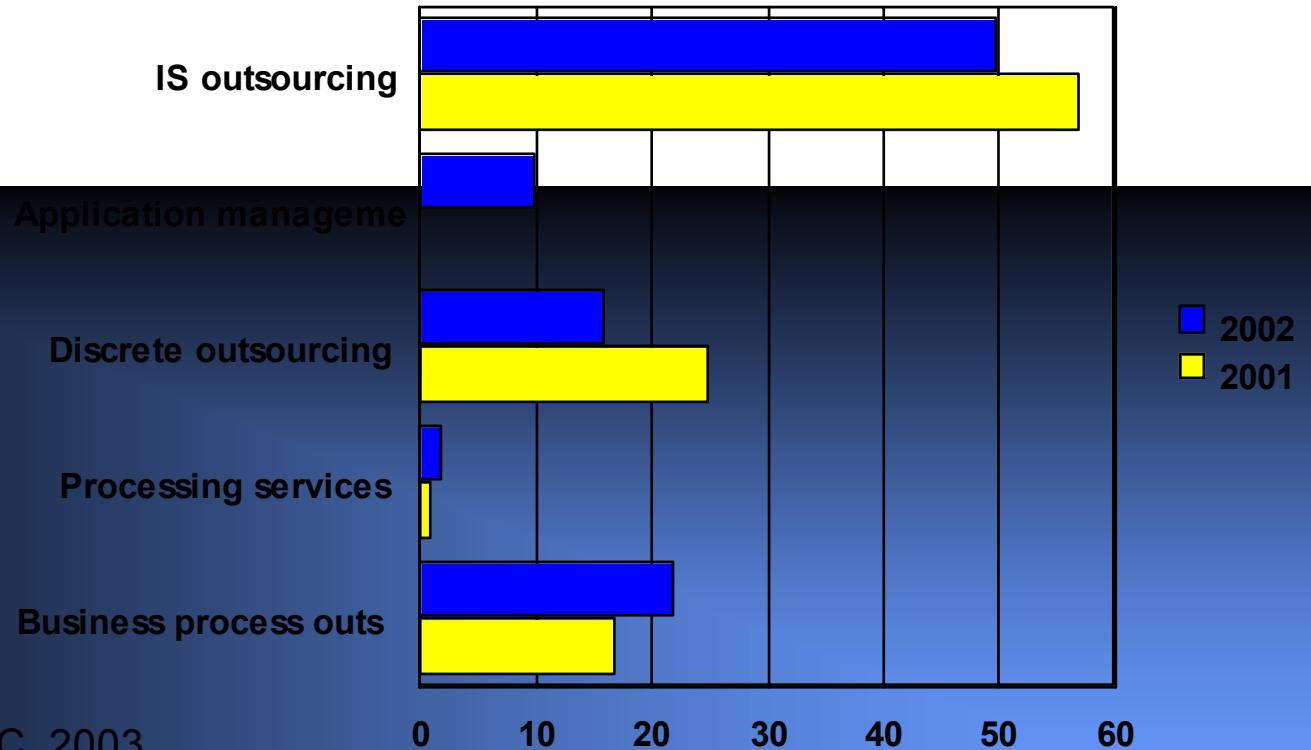
Trend di mercato dell'outsourcing: l'aumento della spesa

Nel prossimo futuro le aziende spenderanno mediamente *un terzo del loro budget nell'outsourcing*, non solo tecnologico, bensì inteso nella sua accezione più ampia



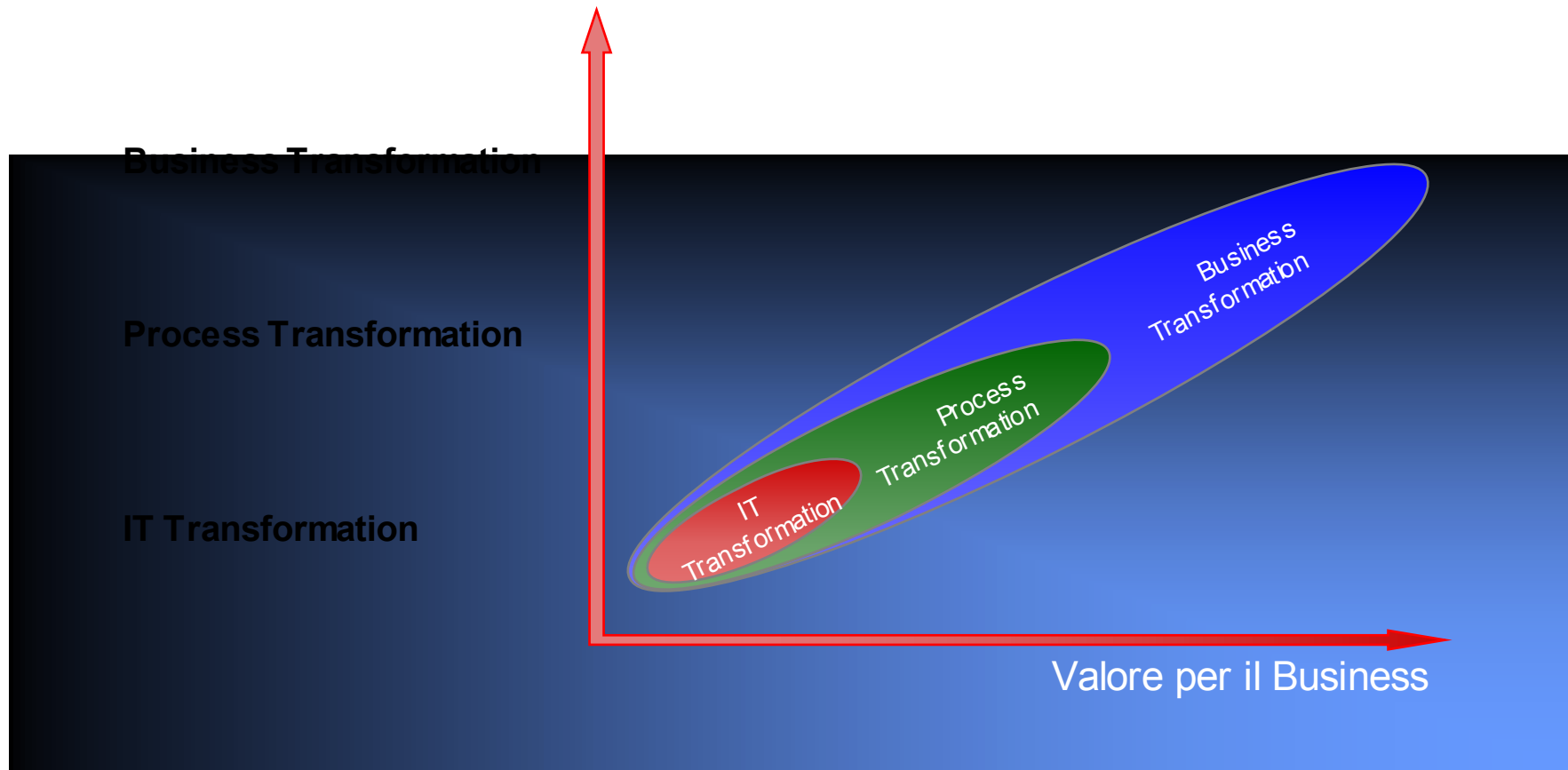
Fonte: Ricerca Michael F. Corbett. I dati di spesa 2002 e 2003 sono stimati

Distribuzione dei contratti di outsourcing: i 100 piu' significativi firmati in Europa nel 2001 e 2002



Fonte IDC ,2003

Il modello di outsourcing evolve: il valore ai clienti passa attraverso la partnership nella trasformazione del business, dei processi e dell'IT.



Per continuare a generare valore le aziende dovranno in futuro evolvere verso modelli di outsourcing focalizzati sul network

Era "on demand"

- Volatilità
- Impossibilità di fare previsioni
- Competizione
- Cambiamenti continui
- Focus sui costi variabili
- Tecnologia = strategia

Business "On Demand"

- Reattivi
- Costi variabili
- Focalizzati
- Resilienti

Bisogni di Business

- Focalizzazione sulle decisioni strategiche
- Ritorno sugli investimenti
- Outsourcing
- Riduzione dei rischi

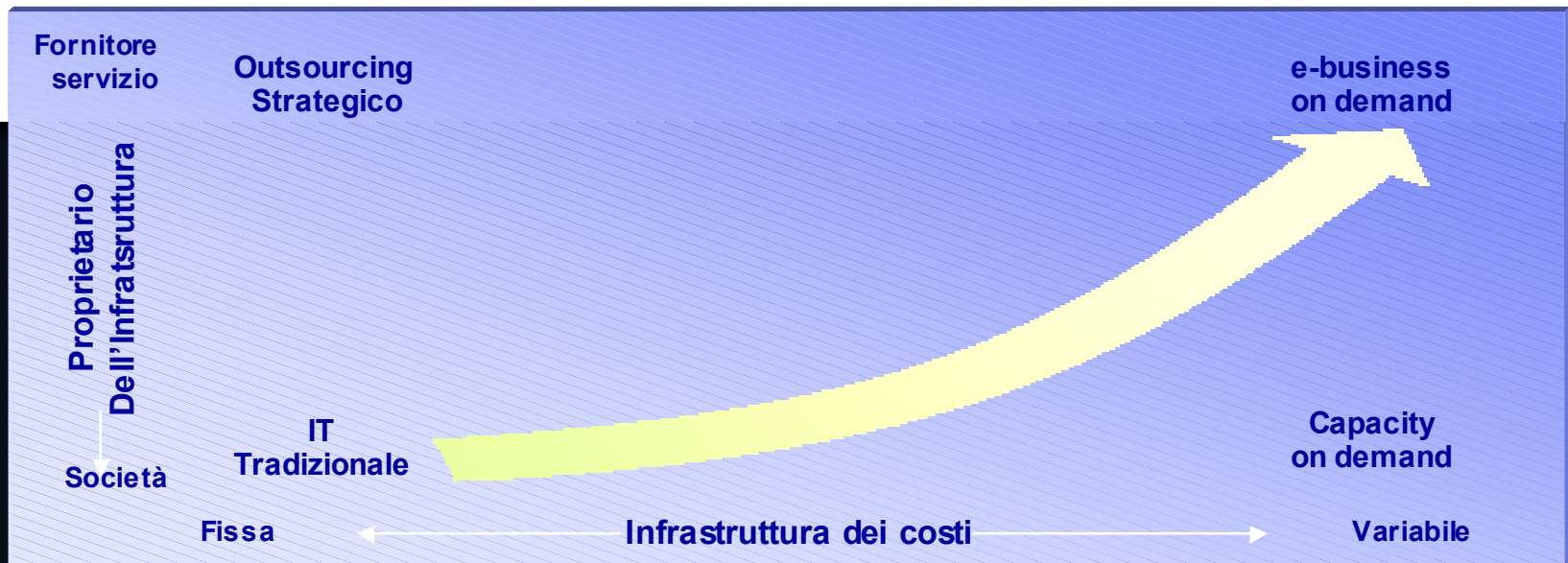
Ottimizzazione del business

Ottimizzazione dell'infrastruttura

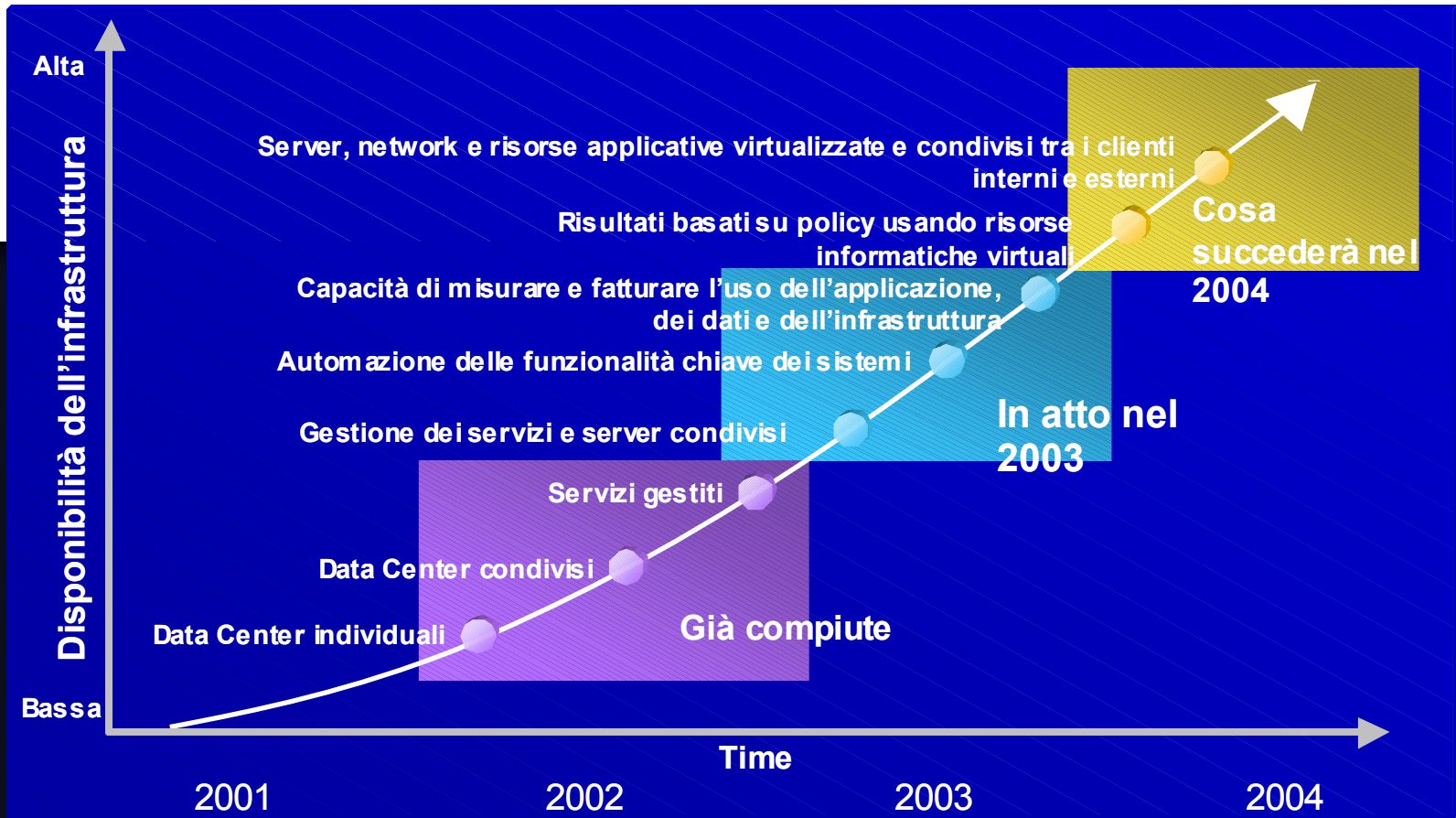
Ambiente operativo

- Integrato
- Basato su standard aperti
- Virtualizzato
- Autonomico

L'ambiente "on demand" offre maggiore flessibilità, struttura variabile dei costi e vantaggi economici rispetto all'acquisto e alla gestione dell'infrastruttura IT

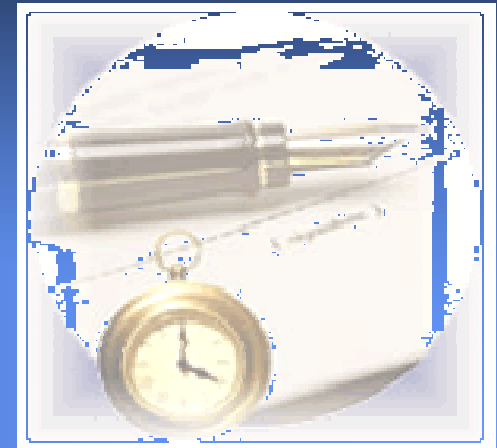


Il modello evolutivo adotta criteri basati sulla disponibilità dell'infrastruttura

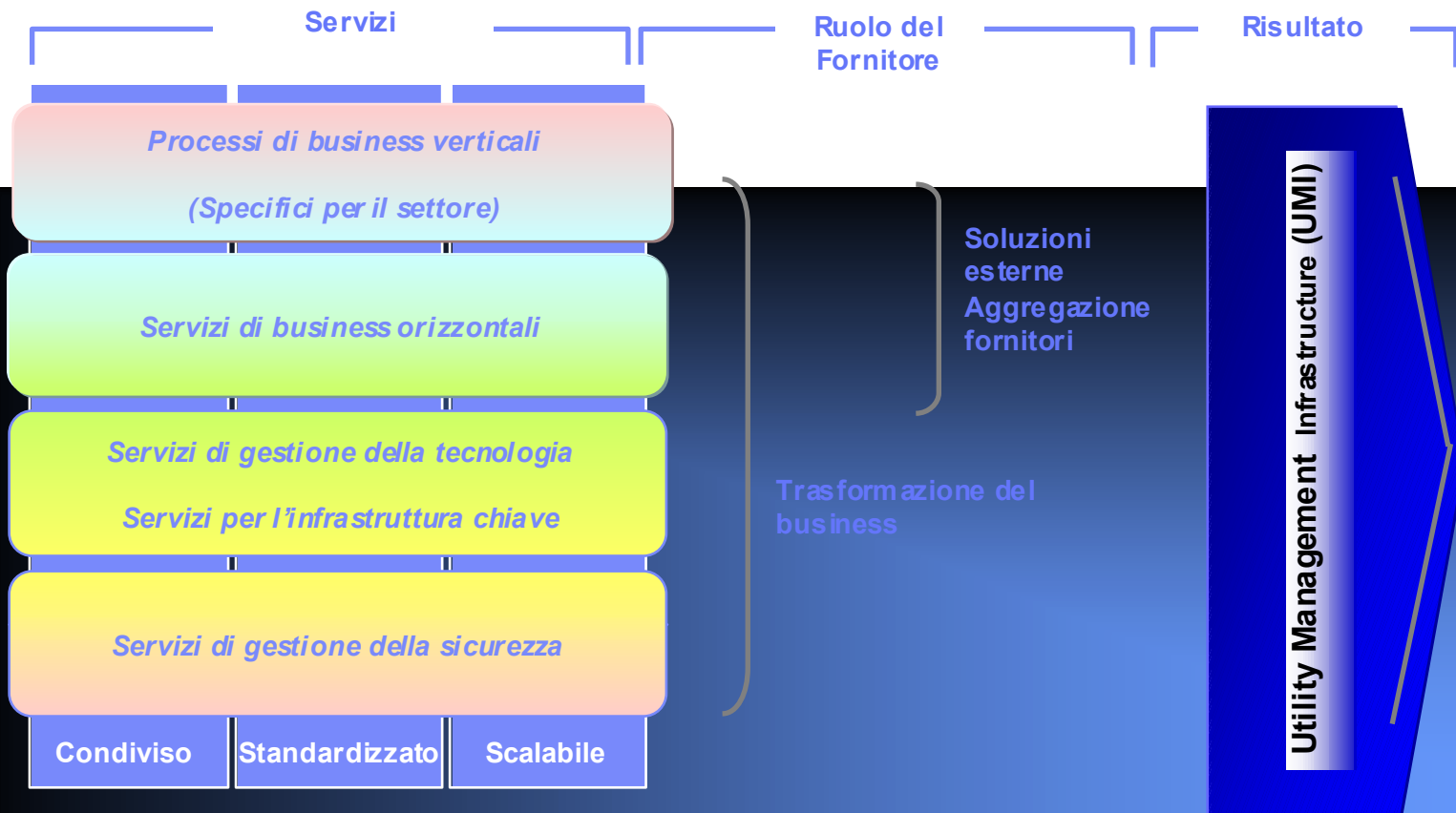


Agenda

1. *Trend di Mercato ed evoluzione nell'Outsourcing*
2. *L'approccio IBM alla sicurezza*
3. *La metodologia e le competenze IBM*

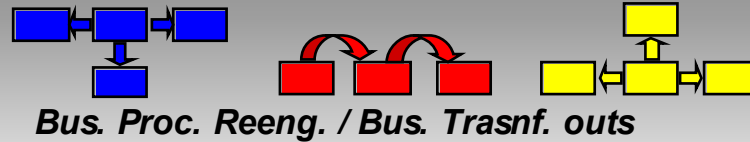


Nel nuovo modello il fornitore di outsourcing deve svolgere diversi ruoli per fornire soluzioni “on demand”



Per realizzare il business on demand servono molteplici competenze, fra cui quelle di sicurezza, che coinvolge ogni aspetto della realtà aziendale sia a livello di business sia a livello IT

Competenze relative al Business del cliente



Competenze di industria
Competenze di processo



Competenze applicative

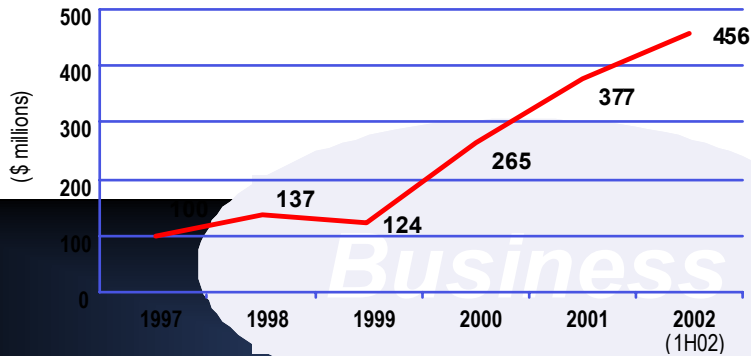


Competenze di tecnologia e di piattaforma



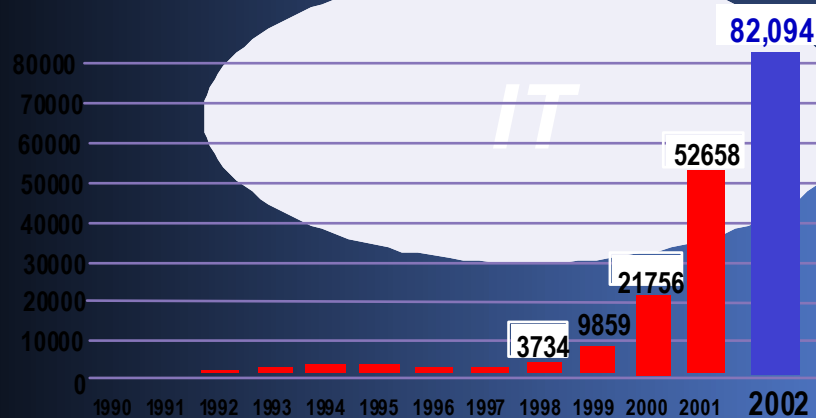
Sicurezza

Oltre ai rischi legati all'esternalizzazione dei servizi, bisogna considerare che l'utilizzo di nuovi modelli di business comporta un forte incremento degli incidenti di sicurezza



Escalation dell' **impatto finanziario** dovuto ad incidenti di sicurezza

Source: April, 2002 CSI/FBI
USA Computer Crime and Security Survey

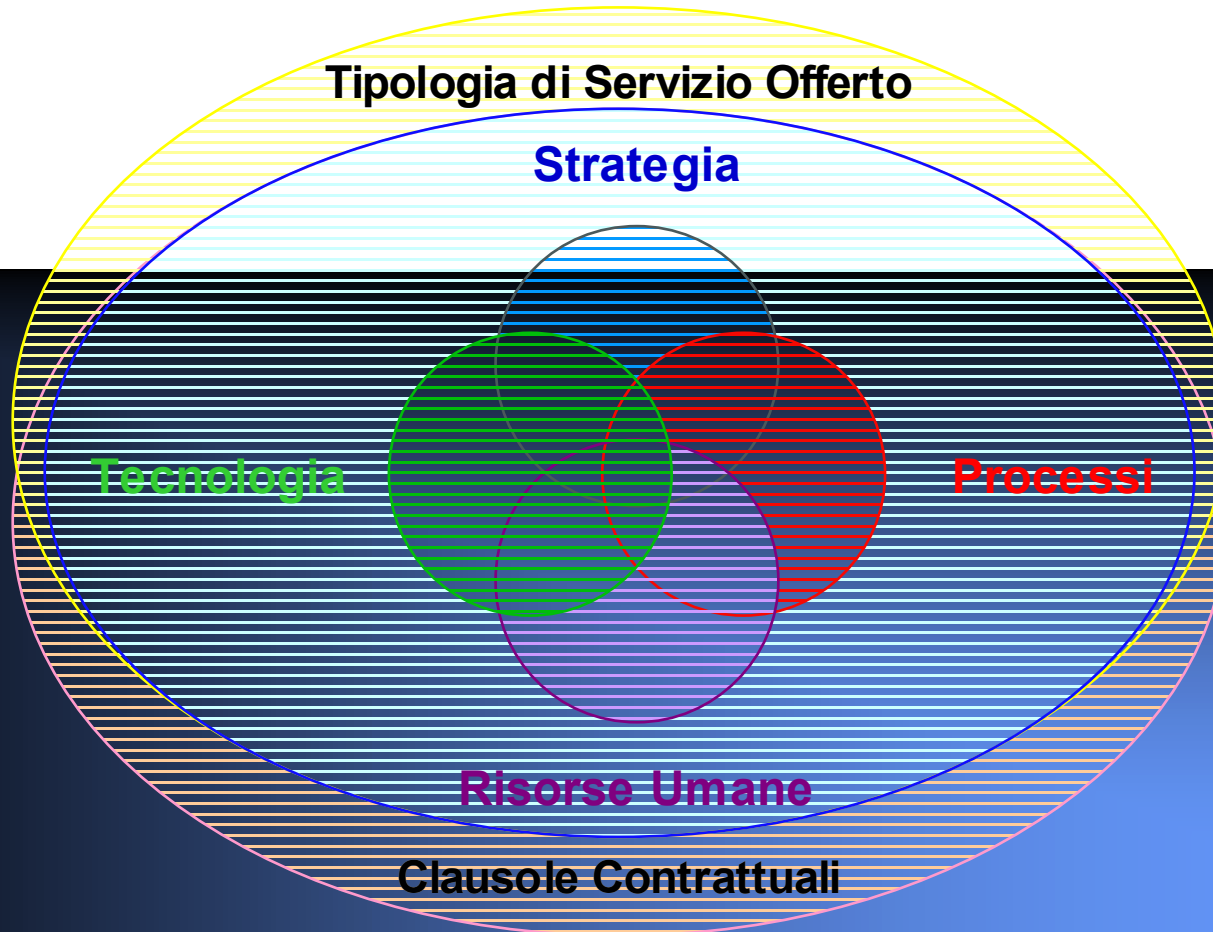


Escalation del **numero di incidenti** di sicurezza informatica

Source: www.cert.org

Sources: IDC, SWG GMV Extensions

La tematica della sicurezza nell'outsourcing richiede un approccio globale, che si articola su strategia, tecnologia, processi e risorse umane, ed è strettamente connesso alla tipologia di servizio offerto e a quanto previsto dal contratto



I servizi di sicurezza offerti dal provider sono strettamente correlati con le tipologie del servizio di outsourcing

- IT outsourcing services – data center;
- Network outsourcing services;
- Network Workstation Management Services;
- Application Management;
- Managed Security Services;
- Customer Service Center;
- Business Recovery Services;
- Trasformational Outsourcing di processi quali:
 - CRM;
 - Security (es.: Security Operation Center)
 - ...

La sicurezza è un aspetto rilevante del rapporto di outsourcing, e pertanto deve essere definita in sede contrattuale

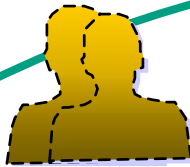
I Service Level Agreement sottoscritti dal cliente e dal fornitore dovranno prevedere:

- Responsabilità di Security, nell'ambito delle specificità del servizio offerto;
- Responsabilità di Privacy, secondo la legge 675/96;
- Il contenuto e le caratteristiche dei servizi base e opzionali inclusi nel contratto;
- I risultati attesi;
- I Key performance Indicators utilizzati per misurare il raggiungimento dei risultati attesi;
- Le modalità di billing, legate ai risultati attesi e ai Key Performance Indicators.

Contract		
IBM	Cust	N/A
	XYZ	
Physical Access Controls		
Physical Security Roles/Responsibilities		
Provide physical security controls at Customer XYZ facilities		
Provide physical security controls at IBM facilities		
Data Center Access		
Restrict access to all data processing areas to authorized personnel only, whether at Customer XYZ or IBM facilities, for which IBM has security responsibility		
Conduct periodic reviews of the data processing areas for which IBM has security responsibility and perform follow-up activities		
Logical Access Controls		
Userids		
During the Transition period, perform a baseline inventory of userids for the systems for which IBM has security responsibility		
Userid Authorization		
Authorization of userids for Customer XYZ personnel		
Authorization of userids for IBM personnel		
Management Notification to Revoke		
Notify the appropriate userid administrator(s) when Customer XYZ personnel no longer need their access		
Notify the appropriate userid administrator(s) when IBM personnel no longer need their access		
Employment Review		
Perform Employment Review for Customer XYZ employees		
Perform Employment Review for IBM employees		
Userid Revalidation		
Revalidation of Customer XYZ userids		
Revalidation of IBM userids		
Resetting Passwords		
Establish the process criteria for resetting user's passwords and disclosing them to authorized personnel (Normal and Deaf/Hearing-impaired as required)		

Particolare attenzione deve essere posta agli aspetti legati alla Privacy, per le implicazioni legali che possono assumere eventuali inadempienze

Responsabile del trattamento



**PERSONA FISICA/
GIURIDICA**
Designato dal Titolare per
esperienza e capacità,
fornisce garanzia del rispetto
delle disposizioni

Incaricati del trattamento



PERSONA/E FISICA
Agisce sotto autorità del
Titolare/Responsabile e attua
le operazioni necessarie per
il trattamento. L'incaricato
deve essere autorizzato al
trattamento dei dati sensibili

Custode delle chiavi



PERSONA/E FISICA
Custodisce le parole chiave per l'accesso ai
dati (password) attribuite agli utenti
oppure
Custodisce le chiavi di accesso agli archivi
cartacei di dati sensibili gestendo il relativo
registro previsto per gli accessi straordinari

Amministratore di Sistema



PERSONA/E FISICA
Sovrintende alle risorse del
sistema operativo di un
elaboratore o di un sistema di
base dati e di consentirne
l'utilizzazione.

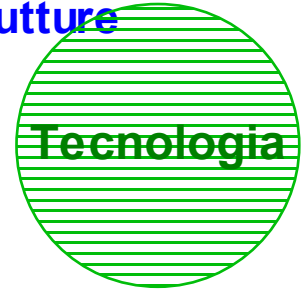
La strategia di sicurezza definisce regole relative alla confidenzialità, privacy, integrità ed accessibilità dei dati



L'outsourcer deve avere un framework organizzativo e normativo condiviso da tutte le funzioni e le strutture coinvolte nel servizio, finalizzato al raggiungimento degli obiettivi di sicurezza fissati nel contratto



La Tecnologia deve garantire sicurezza e continuità delle infrastrutture condivise e il recepimento dei requisiti del cliente



Le sfide principali della sicurezza nel mondo "on demand":

- ④ Integrità' dell'ambiente, oltre che dei dati
- ④ Integrazione con le applicazioni
- ④ Identity integration
- ④ User provisioning
- ④ Resilienza

I Processi permettono di realizzare le strategie di sicurezza attraverso la definizione dei compiti e dei privilegi associati alle figure che operano nell'ambito della sicurezza e dell'IT



I processi IT e di business devono essere rivisti, in un modello di business "on demand", in un'ottica di sicurezza diffusa su tutti gli ambienti

Processi di gestione e amministrazione della sicurezza :

- Accessi alle aree fisiche
- Accessi alla rete e alle applicazioni (gestione utenze, pw, profili, etc.)
- etc.

Processi di controllo e monitoraggio

Processi di gestione degli incidenti

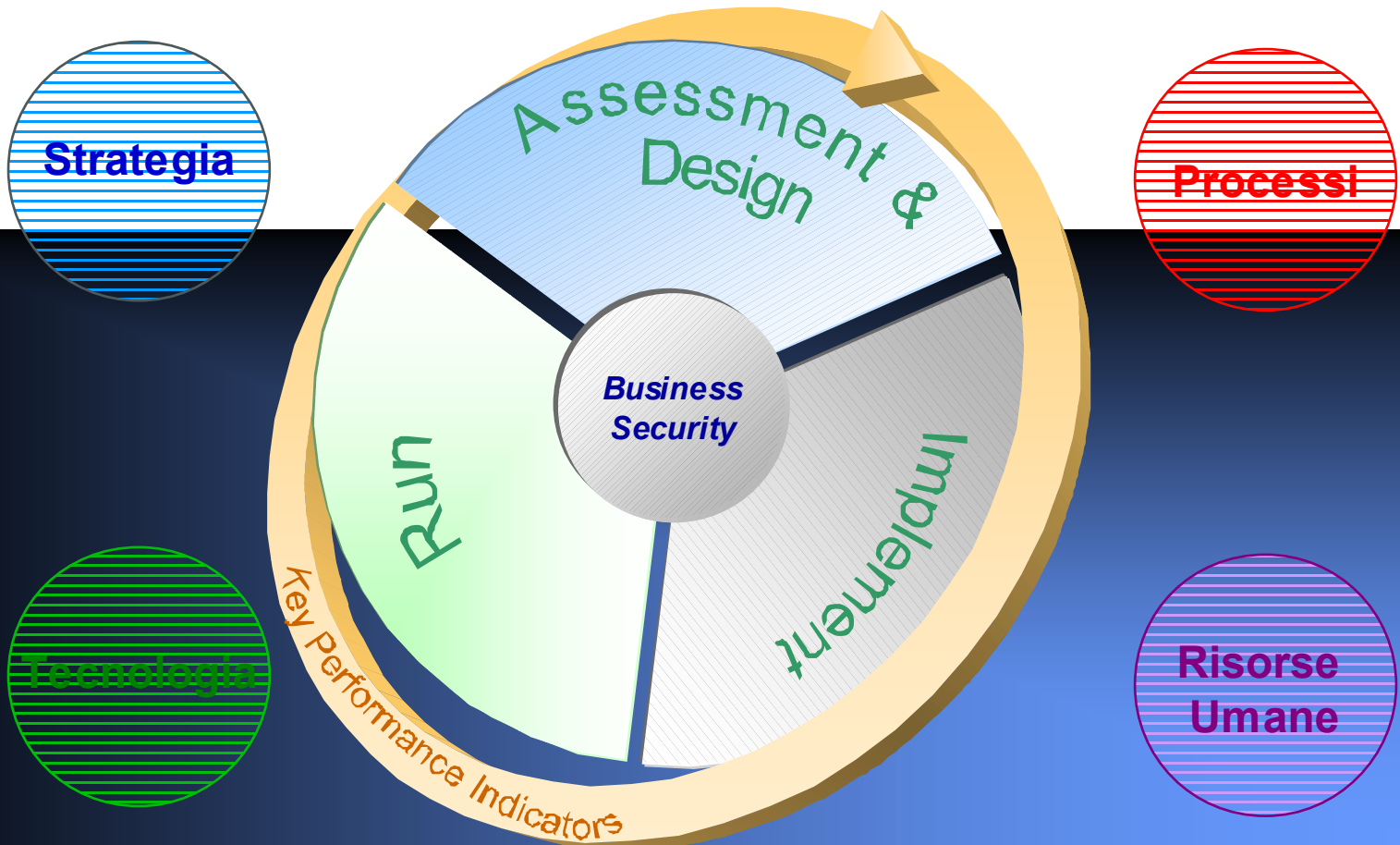
Le Risorse Umane



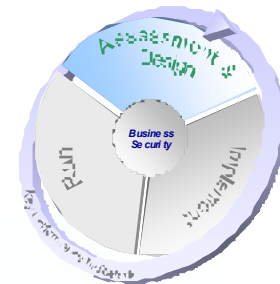
Il personale deve conoscere cosa deve fare per garantire all'azienda e al cliente il soddisfacimento degli obiettivi contrattuali e previsti dalle leggi

- Formazione e sensibilizzazione degli utenti, ad ogni livello organizzativo
- Capacità di rilevare e rispondere tempestivamente ad eventuali incidenti.

L'approccio globale di IBM prevede l'erogazione di servizi secondo un programma in grado di rispondere ad ogni esigenza di sicurezza, sulla base dei principi enunciati

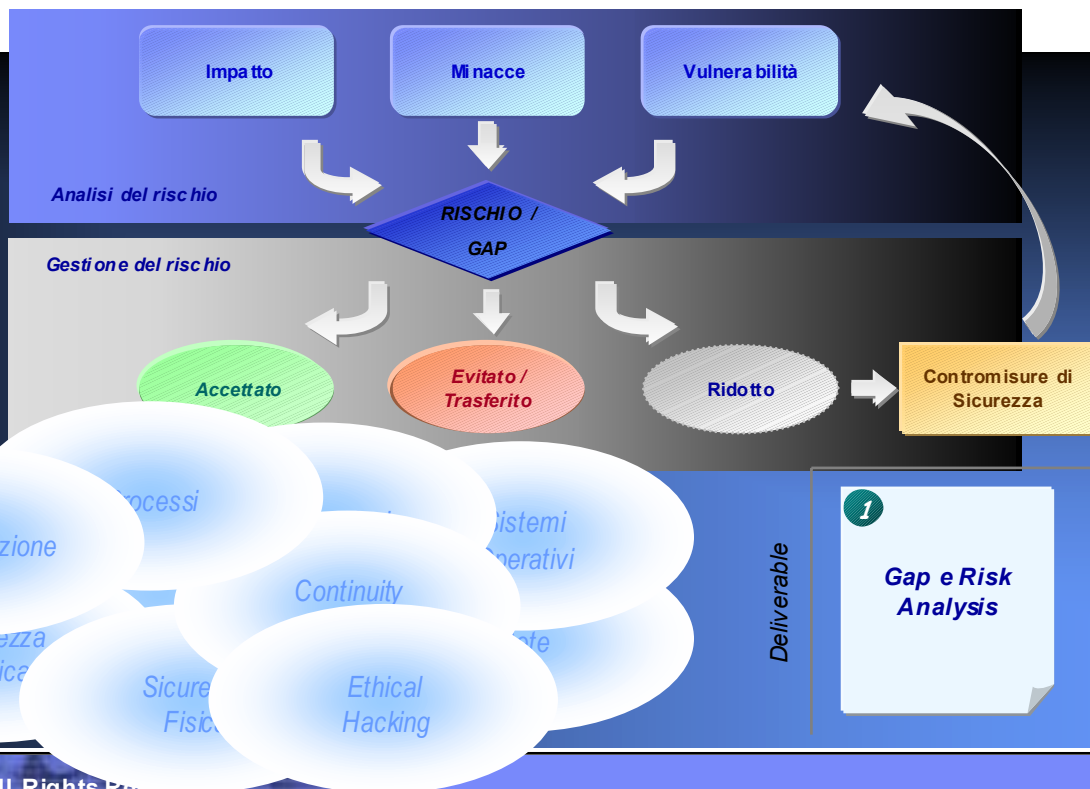


La fase di Assessment & Design identifica la situazione as-is in termini di sicurezza, valuta le necessita' ed il gap rispetto alla sicurezza desiderata e consigliata (servizio base e opzionale)

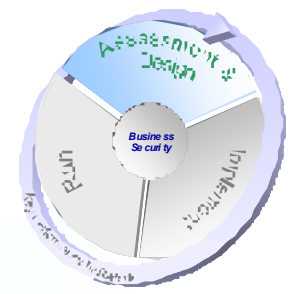


Assessment

Analisi del **livello di sicurezza** garantito alle informazioni e alle risorse informatiche dalle modalità operative aziendali e dai controlli di sicurezza in atto prima del contratto di outsourcing, valutazione dei requisiti di sicurezza e del gap con il livello di sicurezza stabilito nel contratto e conseguente **individuazione delle contromisure** e delle aree di intervento.



La prioritizzazione delle attività fornisce al management aziendale uno strumento decisionale per pianificare gli interventi di sicurezza delle informazioni



Prioritizzazione delle attività

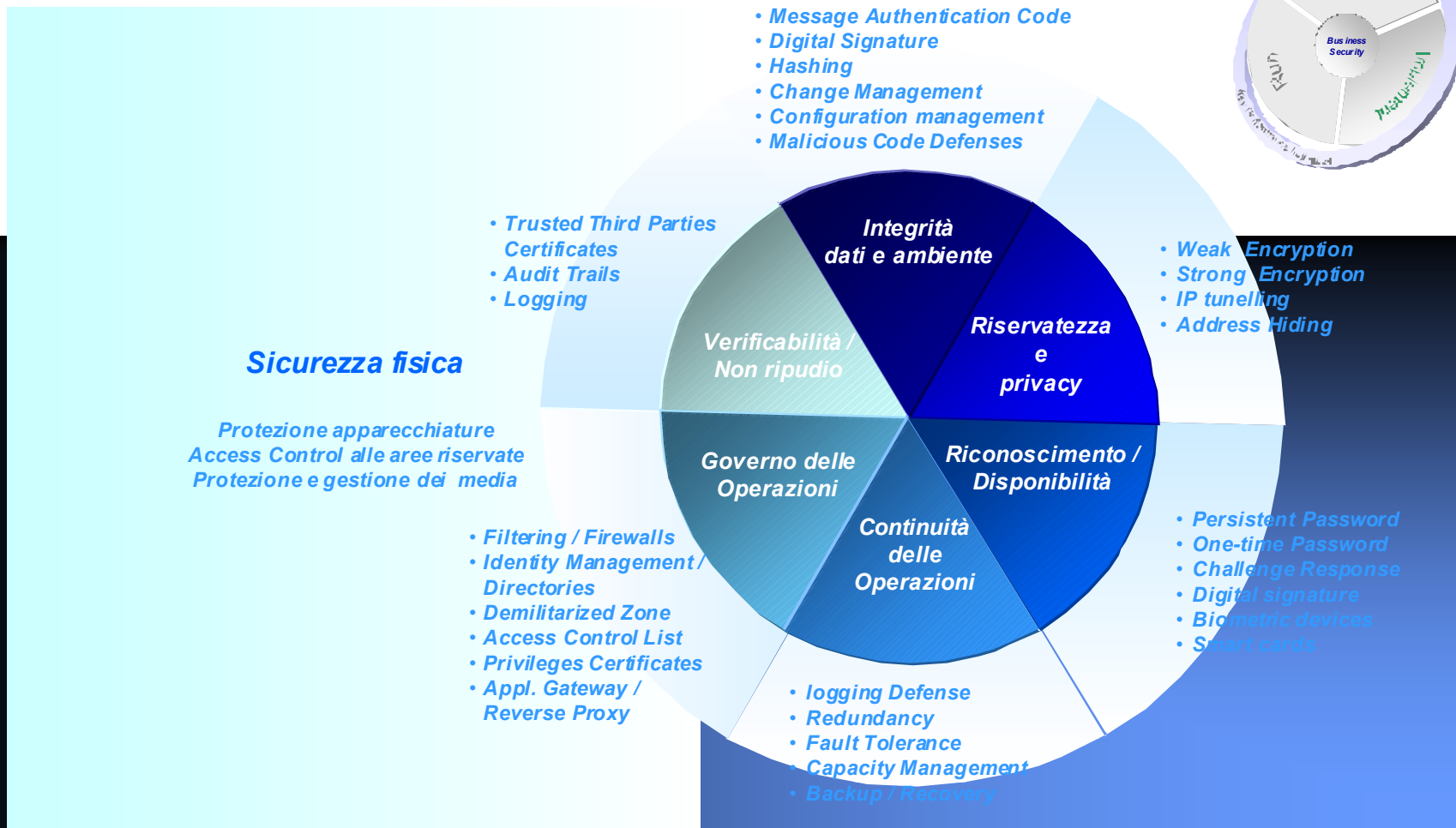
*Ponderazione delle attività necessarie a garantire un adeguato livello di sicurezza aziendale in funzione dei **rischi** evidenziati, dei **costi** delle contromisure connesse, delle **priorità** aziendali e del **benchmarking** sulle aziende di riferimento del settore di appartenenza*

Attività previste

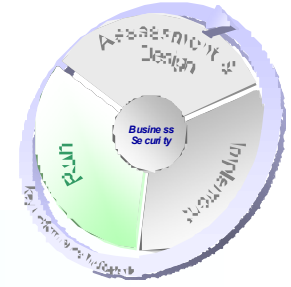


Deliverable

La selezione dei prodotti/soluzioni deve indirizzare le esigenze di protezione, di monitoraggio e di controllo dei dati, dei sistemi e delle reti



I Managed Security Services permettono alle aziende di poter dedicare le competenze interne ad attività a maggior valore e ridurre i costi fissi infrastrutturali



Managed Security Services

Outsourcing dei servizi di gestione e amministrazione della sicurezza informatica dei diversi ambienti aziendali (web, rete, server, pdl) garantendosi un adeguato livello di servizio e immediata (e efficiente) risposta a fronte di incidenti

Servizi

Provisioning informazioni associate all'utente sui sistemi (Utenze, LDAP; ...)

Amministrazione delle informazioni utenti

Esecuzione e controllo procedure di configurazione sistemi e firewall

Gestione cambiamenti configurazioni di sistema

Esecuzione e controllo procedure di backup e recovery

Gestione dei salvataggi

Gestione dell'antivirus

Supporto operazioni sicurezza on site su PDL o server

Ethical Hacking

Health Checking

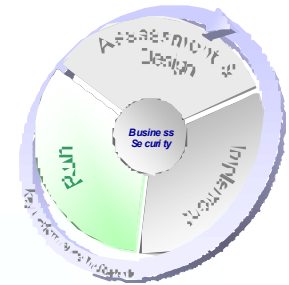
Monitoraggio dei sistemi e della rete

- **Intrusion detection System (Network + Host)**
- **Firewall Management**

Incident Handling

Education

La gestione in outsourcing delle attività di Business Continuity e Recovery garantisce alle aziende l'appropriata continuità del proprio business



Servizi di Business Continuity & Recovery

Gestione e manutenzione delle attività necessarie a garantire il livello di continuità adeguato alle esigenze aziendali di business demandando a terzi i costi fissi connessi alle strutture fisiche e allo sviluppo delle competenze necessarie

- **Total Continuity Management Programs**
- **Recovery Incident Management**
- **Crisis Management Services**

- **E-business Continuity**
- **ERP Continuity**
- **Call Center Continuity**
- **Custom Application Continuity**

- **Recovery Script writing**

- **IBM Platform recovery**
- **Multi-vendor Platform Recovery**
- **Network Recovery**
- **Workgroup Recovery**

Business Continuity Managed by IBM

Critical Business Process Continuity

IT Recovery Assessment and Planning

Multi Vendor IT recovery

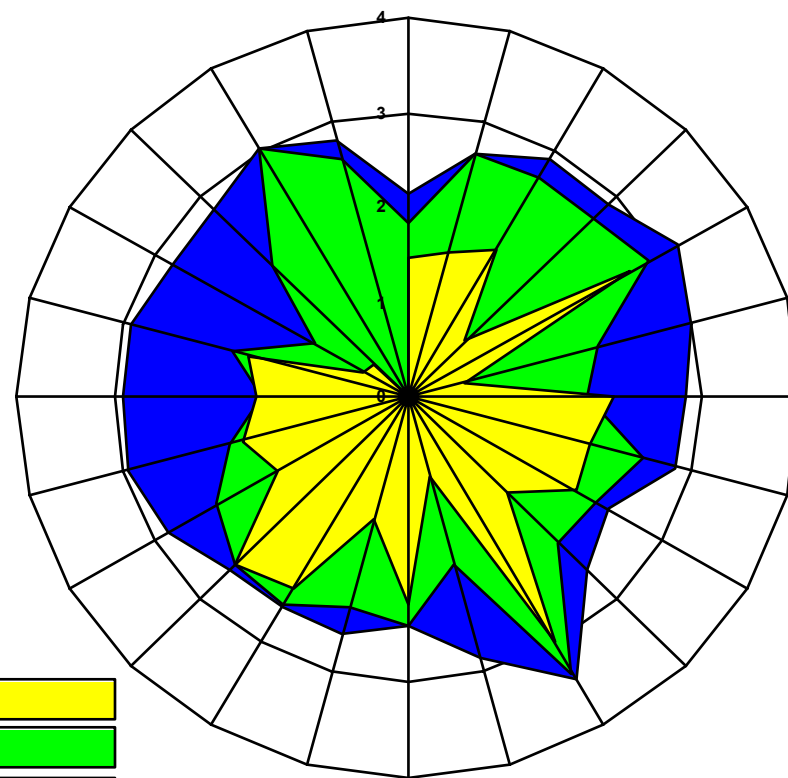
Run



La gestione della Sicurezza delle informazioni rientra all'interno del processo di IT Governance aziendale e richiede un sistema di misurazione

Modalita'

Individuare i Key Goal/Performance Indicator più opportuni attraverso i quali definire i livelli target di sicurezza ed effettuare le misurazioni dei processi più significativi



Situazione attuale



Soglia minima desiderata dall'azienda

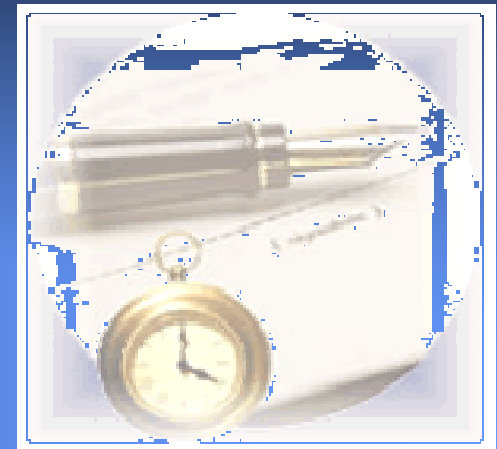


Copertura ideale per il settore d'appartenenza

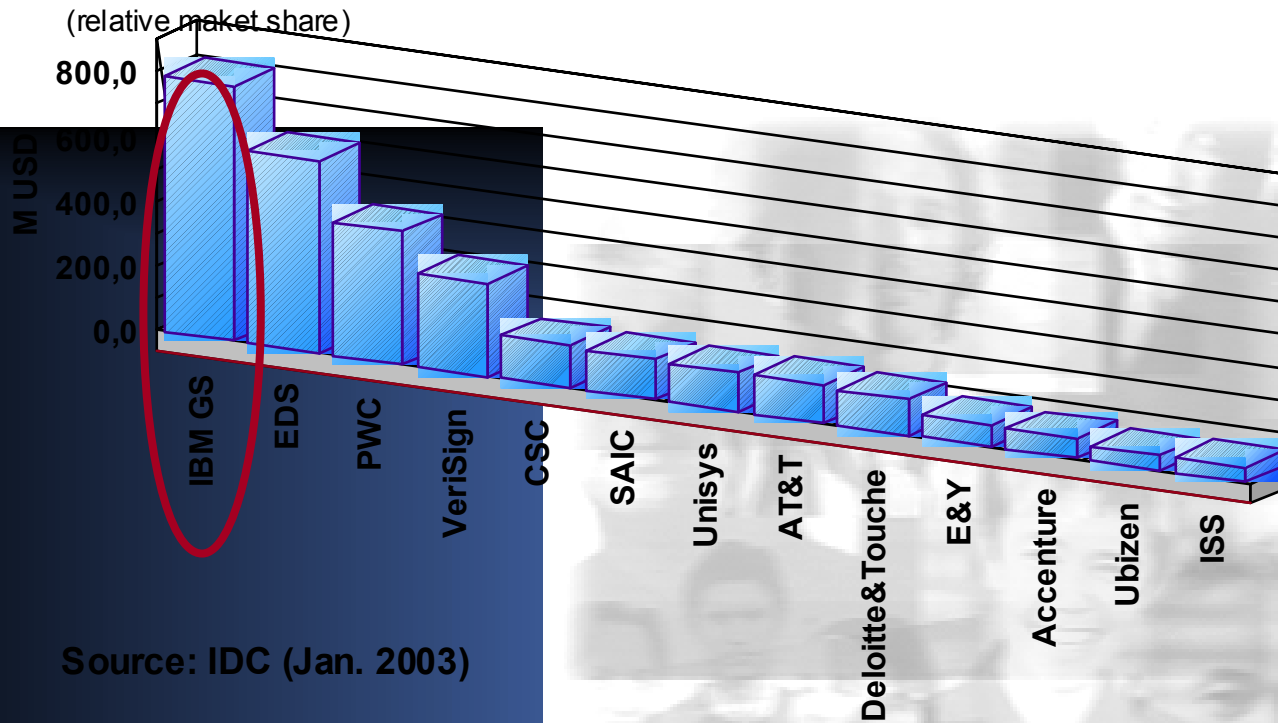


Agenda

1. *Trend di Mercato nell'Outsourcing*
2. *L'approccio IBM alla Sicurezza*
3. *La metodologia e le competenze IBM*

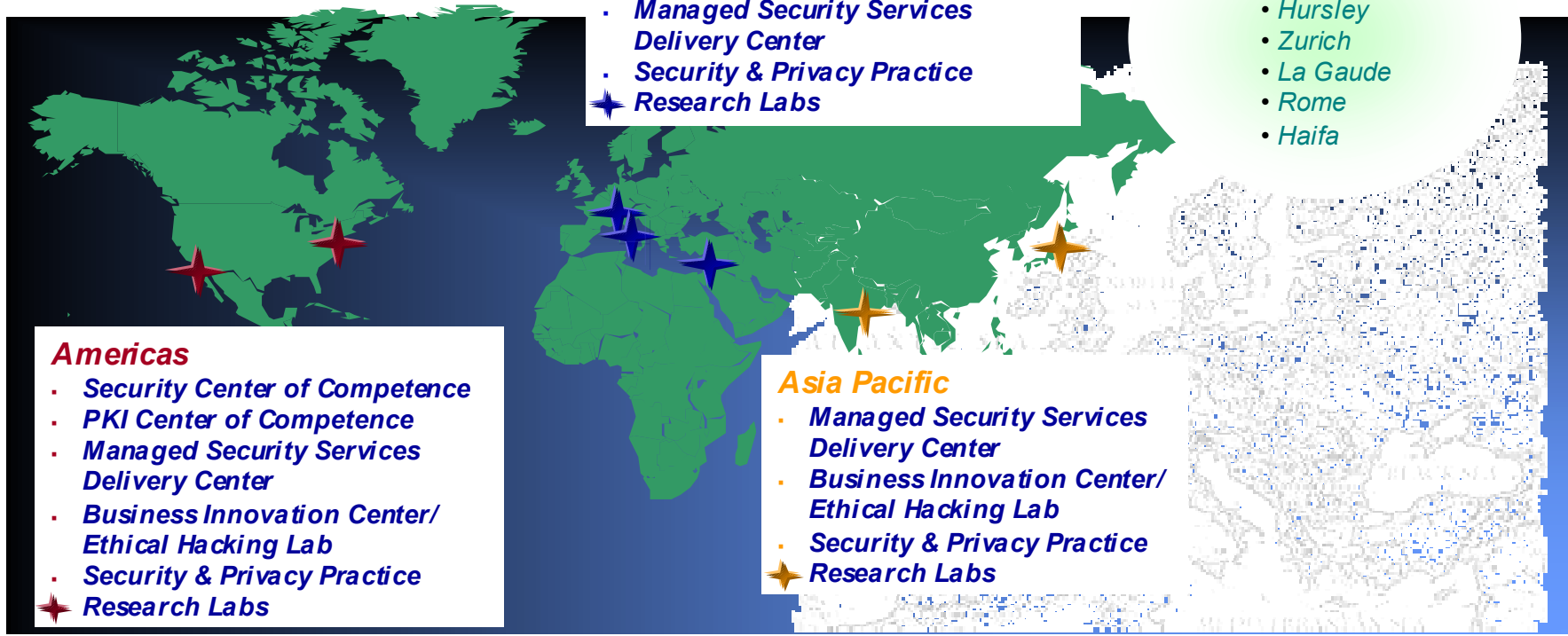


IBM è leader mondiale indiscusso nella fornitura di Servizi

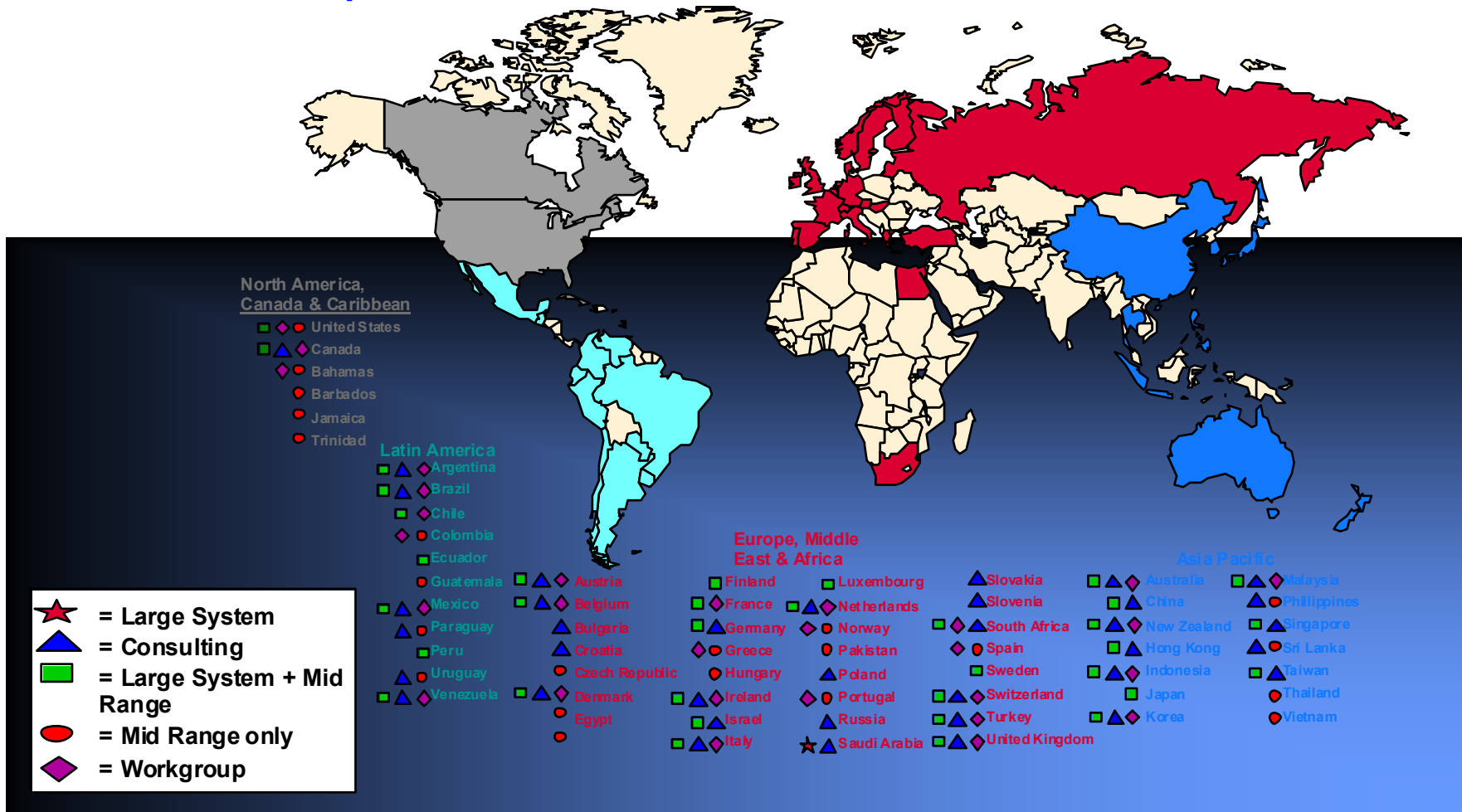


IBM Security & Privacy Services è una solution area IBM a livello world wide: centri di competenza e laboratori di ricerca sono presenti in tutto il mondo compresa l'Europa

Competenze specifiche, esperienze multisettoriali e risorse a disposizione, nel mondo e in EMEA, costituiscono i principali punti di forza dei team di lavoro IBM, **la più grande comunità sulla sicurezza a livello mondiale, 3.000 specialisti** di sicurezza che lavorano come un unico team e in maniera globale

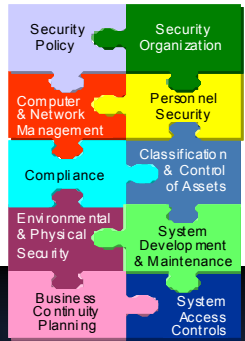


IBM dispone di una rete capillare di centri di recovery distribuiti a livello mondiale attraverso i quali fornire servizi in grado di garantire la continuità delle operazioni di business dei clienti



IBM affronta i temi della sicurezza basandosi su standard internazionali integrandoli con i propri asset e metodologie

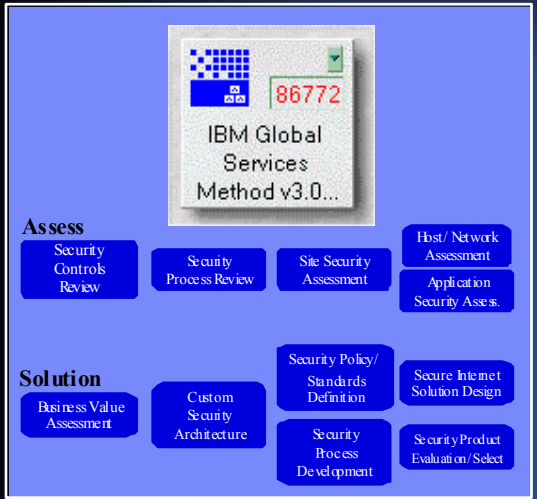
BS7799
IEC/ISO 17799



Intellectual capital



IBM GS Method



US TCSEC
Trusted Computer System Security Evaluation Criteria



CTCPEC
Canadian Trusted Computer Product Evaluation Criteria



ITSEC
Information Technology Security Evaluation Criteria

V 1.0 - 1996
V 2.0 - 1998

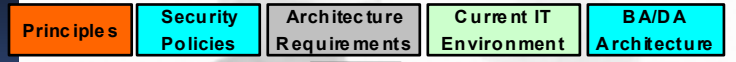


<http://cs.rncsl.nist.gov>

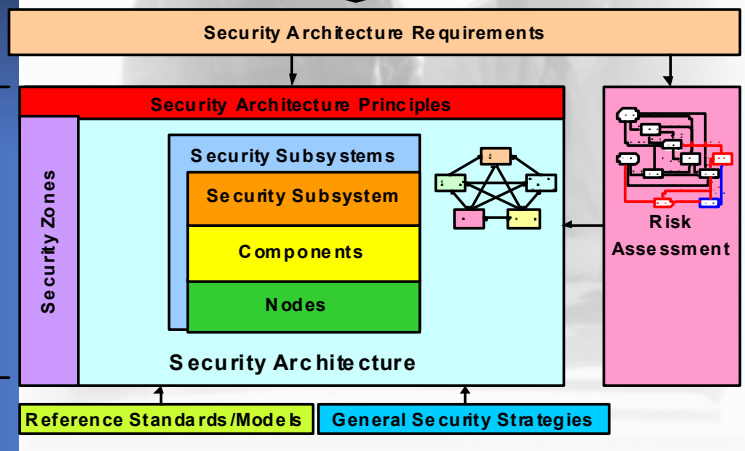
V 2.01 - 1999

ISO/IEC 15408

Architecting Secure Solution



Inputs



Functional Design



Mariangela Fagnani
Security & Privacy Services
e-mail - mfagnani@it.ibm.com
tel. +39.02.5962.0150
mob. + 39.335.7248724

Grazie



All Rights Reserved

IBM affronta anche la sicurezza delle informazioni in ottica di creazione di valore per i propri clienti, disponendo di un approccio globale End To End

