Dalla governance alla gestione degli incidenti passando per la BIA e per la gestione dei rischi

Dagli standard al caso reale

Di cosa parleremo

- Scenario di riferimento sulla base degli standard
- Trend e soluzioni disponibili
- Case study (approccio top-down vs approccio bottom-up)

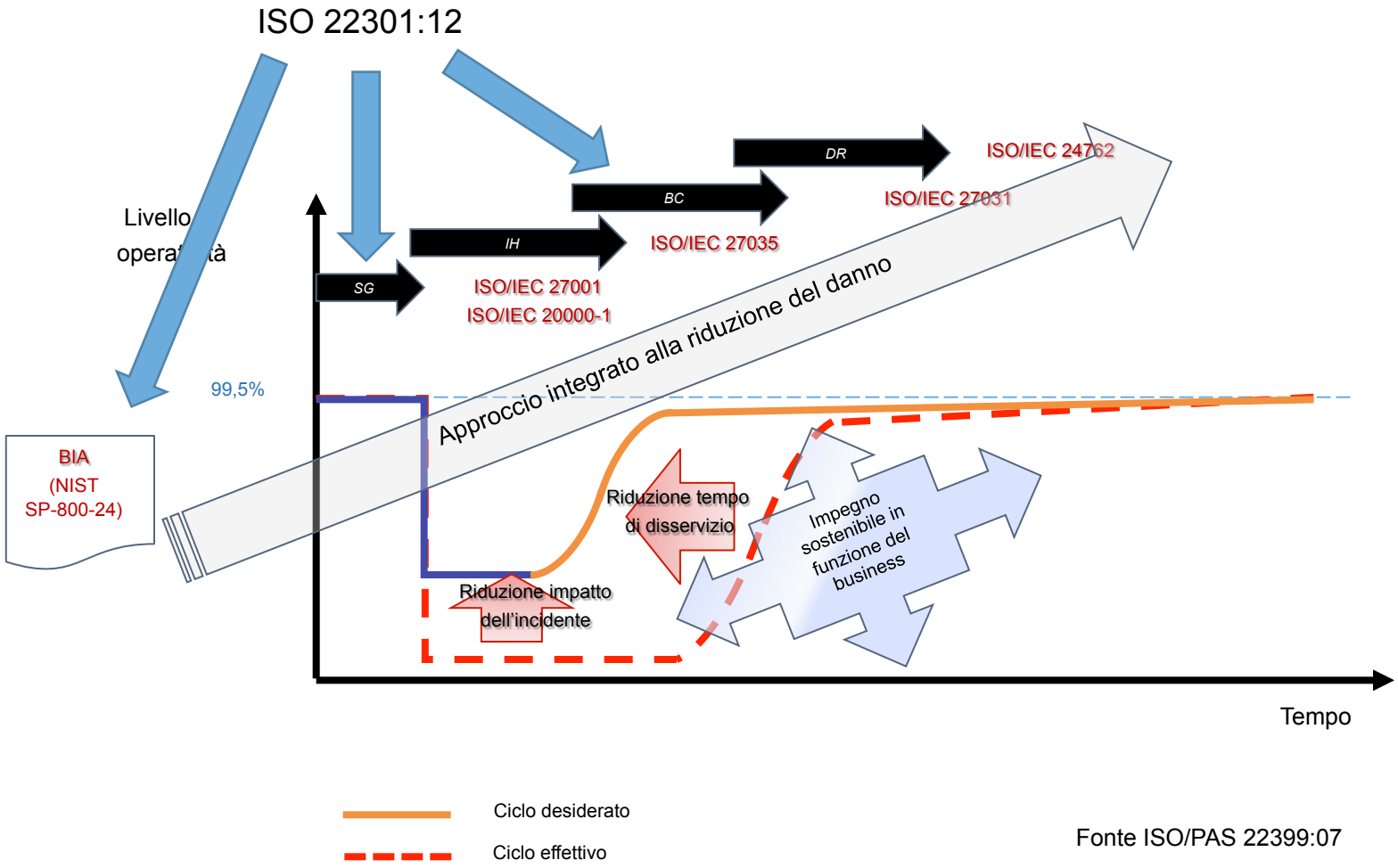
Scenario di riferimento sulla base degli standard

- Complessità degli scenari di business
- Offerta di servizi e soluzioni infinite
- Supply chain sempre più lunghe ed articolate
- Contrattualistica variabile
- Risultati non sempre in linea con le attese ed aspettative iniziali

Scenario di riferimento sulla base degli standard

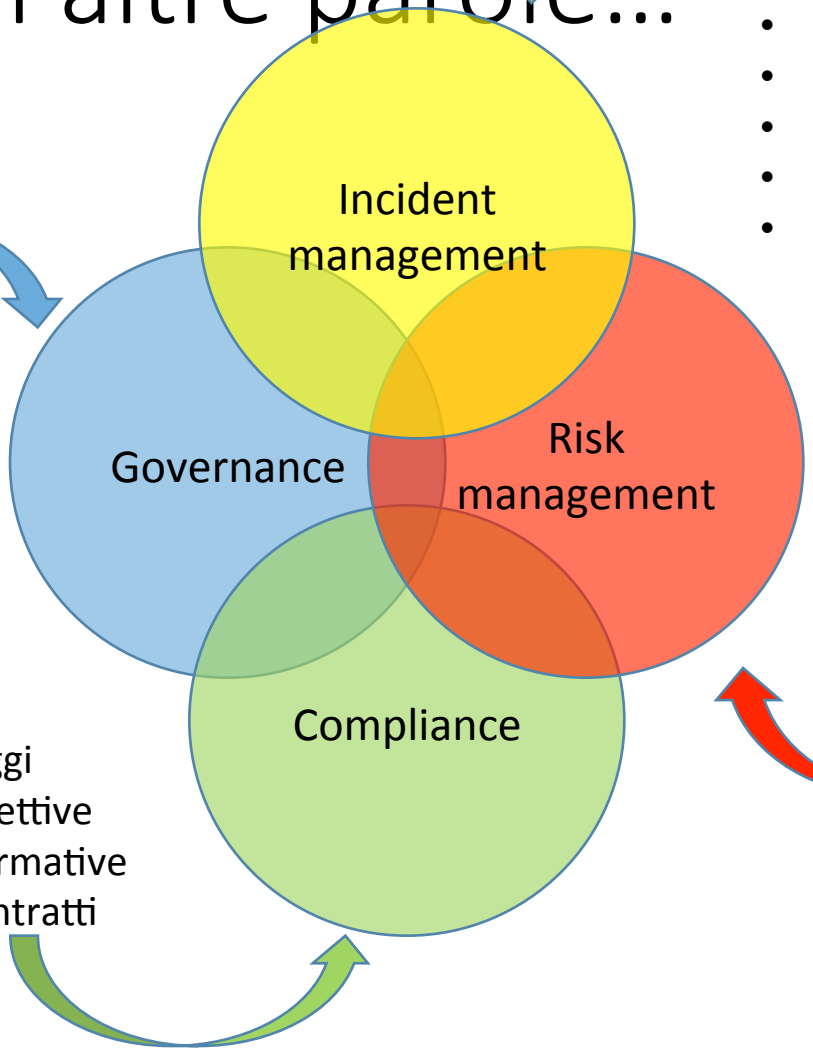
- Uno dei maggiori problemi è l'allineamento tra la governance, la compliance, la gestione dei rischi e la gestione dei ritorni «dal campo»

Scenario di riferimento sulla base degli standard



Fonte ISO/PAS 22399:07

In altre parole…



- Sistemi di campo
- SCADA
- VA/PT
- Incidenti/eventi
- BC/DR

- Esigenze
- Strategie
- Politiche
- BIA

- Valore informazioni
- Impatti e probabilità incidenti
- Rischio accettabile
- Rischio residuo
- Contromisure

- Leggi
- Direttive
- Normative
- Contratti

Trend e soluzioni disponibili

- Standard
  - ISO
  - NIST
  - SANS
  - proprietari
- Certificazioni
  - Proprietarie (ITIL, CISA/CISM, PCI…)
  - ISO (*non tutto è certificabile e da certificare!*)
- Metodologie
  - Proprietarie
  - Pubbliche (su sito ENISA https://www.enisa.europa.eu/)
  - …

Trend e soluzioni disponibili

- Verifiche
  - Organizzative
    - Assessment
    - Audit
  - Tecniche
    - Vulnerability Assessment
    - Penetration test
    - BCP/DRP
    - …
- Tools
  - Proprietari
  - Associati al service desk
  - Innovativi

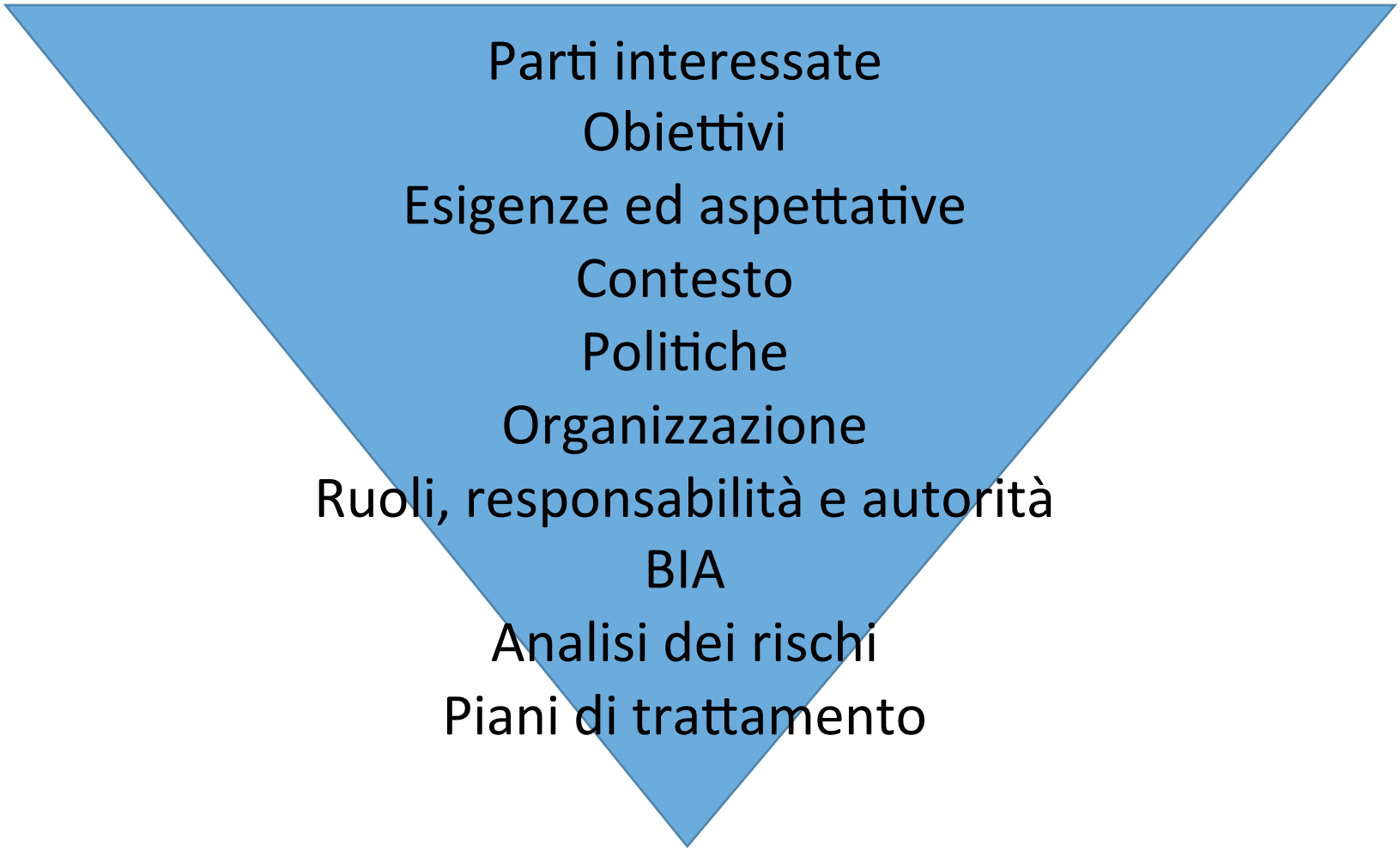
Case study (approccio top-down vs approccio bottom-up)

- Top Down
  - Obiettivi
    - Strutturare un modello articolato partendo da fattori strategici e di governance
  - Vantaggi
    - Fortemente orientato al business
    - Legato a fattori economico finanziari
    - Basato su progetto di Direzione
  - Svantaggi
    - Tempi lunghi (principalmente per scarsa disponibilità attori principali)
    - Scarsa granularità
    - Grado di astrazione
  - Quando applicarlo
    - In presenza di forte committment
    - Necessità di elevato coinvolgimento del top management
    - La sicurezza è un fattore strategico o vincolante del mercato
    - I potenziali impatti implicano perdite rilevanti

Case study (approccio top-down vs approccio bottom-up)

- Bottom Up
  - Obiettivi
    - Strutturare un modello partendo dai fattori operativi
  - Vantaggi
    - Fortemente operativo
    - Tempi rapidi
    - Elevata granularità
  - Svantaggi
    - Scarsamente legato a fattori strategici e di business
    - Scarsa visibilità da parte del top management
    - HW/SW oriented più raramente services oriented
  - Quando applicarlo
    - In presenza di scarso committment
    - Necessità di dimostrare al top management stato della sicurezza
    - Giustificare investimenti per la sicurezza
    - La sicurezza è un fattore tattico-operativo non vincolante per il mercato
    - I potenziali impatti implicano perdite importanti ma non determinanti

Case study (approccio top-down vs approccio bottom-up)



Case study (approccio top-down vs approccio bottom-up)

Case study (approccio top-down vs approccio bottom-up)

- Viste dal lato di un auditor indipendente:
  - Top Down
    - Meno tecnicismo
    - Più legate al business
  - Bottom Up
    - Meno business oriented
    - Più efficaci

E se le sovrapponessimo?

Il caso studio

- Azienda SpA – proprietà di ente patrimoniale
- CdA, AD, DG, DT, Resp. funzioni (rete, DB, progettazione e svilupo ecc.), Resp. Servizi, Help Desk (5x8 on line, after hours, NBD)
- Gestione totale ICT x l'ente patrimoniale (inclusi trusted services)
- 50 dipendenti in totale
- HQ Roma
- Siti secondari non presidiati (RM e MI)
- Organizzazione con processi consolidati (ISO 9001 da oltre 5 anni)
- Tipologia clienti:
  - fortemente vincolati da leggi e direttive
  - scarsamente propensi all'ICT
  - meno di 10.000 clienti diretti
  - Tutti i cittadini italiani come clienti indiretti

Il caso studio

- Il problema
  - adottare un approccio integrato alla sicurezza delle informazioni come fattore strategico
- La soluzione
  - AD e DG approccio top down (fogli excel – valutazioni qualitative proprietarie)
  - DT e resp. approccio bottom up (basato su tool – valutazioni quantitative basate su standard)
- Tempi
  - 3 mesi solari
- Risultato
  - Perfetta coincidenza della valutazione finale (grado di rischio maggiore su disponibilità del servizio PEC)

Il caso studio

		Servizio PEC						
Parte interessata[1]	Interna Esterna	informazioni	È influenzata dal SGSI di XXX SpA (A)			Influenza il SGSI di XXX SpA (B)		
YYY (azionista e committente)	E		X			X		
		• Contenuto casella • Tenuta ricevute • Dati di account • Tenuta dei log • Certificato Gestore	R 5x1	I 5x1	D 5x3	R 3x2	--	D
Cassa Naz. YYY (azionista)	E	• NA	--			--		
Consiglio Distrettuale (Il presidente)	E		X			X		
		• NA	R	I	D	R	--	--
Utenti	E		X			X		
		• Contenuto casella (messaggi) • Tenuta ricevute • Doc. Identità • Dati di account (id e pwd) • Tenuta dei log	R 5x1	I 5x1	D 4x3	R 3x2	--	--
AgID	E		--			X		
		• Tenuta dei log • Certificato Firma Gestore	--	--	--	R 4x1	-- 	D 4x1
Archivi	E		X			X		
		• NA	R	I	D	R	--	D
Terzi interessati ai servizi XXX SpA	E		X			--		
		• Ricevute • Log Servizio	R 5x1	I 5x1	D 4x3	--	--	--
Fornitori	E		X			X		
		• Ricevute • Log Servizio	R 5x1	I 5x1	D 4x3	R 3x2	I 3x1	D 3x1
Top Management XXX SpA (CdA, AD, DG)	I		X			X		
		• Contenuto casella • Tenuta ricevute • Dati di account • Tenuta dei log • Certificato Gestore	R 5x1	I 5x1	D 5x3	R 4x2	I 4x2	D 4x2
Personale XXX SpA (utenti interni)	I		X			X		
		• NA	R	I	D	R	I	D

Valutazione TOP DOWN
AD+DG
BIA + Risk Assessment
Metodologia proprietaria
Quali-quantitativa

Il caso studio

Risk Assessment Report

Posta Elettronica Certificata

Risk	RISCHIO	IMPATTO SU R - I - D - BC	CONTROMISURA ESISTENTE	IMPAT.	FREQ. ACCAD	Rischio	RISULTATO - AZIONE
70	SUN CENTERA (Database log archiviati a norma file system): rischio perdita del database per corruzione file system con indisponibilità dei log con violazione di requisito cogente.	☐ R ☐ I ☑ D ☑ BC	Duplicazione degli apaprati	10	3	30	RISCHIO ELEVATO TRATTARE

Valutazione BOTTOM UP
DT+Funzioni
BIA + Risk assessment
Tool proprietario
Basata su standard
Quantitativa

Il caso studio

- Esito del confronto
  - La disponibilità delle informazioni, inerenti il servizio PEC, raccoglie i maggiori rischi da ambo le valutazioni.
  - La ridondanza potrebbe costituire una contromisura non sufficiente???
  - Avviate ulteriori analisi e valutazioni di contromisure alternative per il trattamento del rischio (in corso verifiche di efficacia)
- **Lessons learned**
  - *Indipendentemente dall'approccio adottato, se questo è basato su un modello organizzativo consolidato e condotto in modo verificabile secondo standard internazionali, le valutazioni tendono a coincidere sebbene generate da posizioni (e viste) diverse*

Fabrizio Cirilli - *fabrizio.cirilli@pdca-srl.it*