

A Consultant Survival Guide

Dalla Corporate alla PMI:

come fare valutazioni, assessment,
auditing, certificazioni, progetti e raccontarlo

(a cura di **Natale Prampolini**, LA ISO27001, CISA, CISM, ITIL)

INDICE DELLA PRESENTAZIONE :

- Esperienze
- Mercati
- Standard e Norme
- Fare / Non Fare
- IT Governance e il Rating dell'Elefante
- Q&A

Come affrontare la valutazione complessiva dell'IT aziendale: le tre domande chiave.

- L'esperienza di circa 219 tra offerte, progetti, risposte a bandi di gara, assessment, valutazioni e certificazioni, tra PA, Telco, Finance, PMI e System Integrators negli ultimi 4 anni.
- Viene sempre più richiesto di fare valutazioni sui servizi IT di aziende in tempi brevissimi, e valutare costi di progetti e produrre offerte in tempi ancora più brevi.
- Quali sono i livelli di maturità IT dei settori industriali.
- Come utilizzare ISO27001, CobiT, Sarbanes-Oxley, ITIL, e il resto della banda.
- Consigli pratici dal campo: cosa fare e soprattutto cosa non fare.
- Il mio metodo di "rating" IT: le tre domande.

Ogni cosa va vista nel suo ambiente

Albert Einstein disse alla sua segretaria: "Queste sono le nuove prove d'esame."

La segretaria: "Herr professor, sono le stesse dell'anno scorso."

Albert Einstein "Ma io mi aspetto risposte diverse."

- **P.A.C. e P.A.L.: 98 risposte a Bandi di gara**
 - Progetti HW e SW
 - Poco tempo, forte accento su:
 - Costi
 - Aspetti tecnici
 - Tempi:
 - impegno: da 2 a 200 gg/uomo
 - calendario: da 2 a 60 giorni

- **D.Lgs 196/03: Protezione dei dati personali**
- **18 DPS + consulenza**
- Aziende Sanitarie, PMI, Servizi, Finanza
 - Redazione e adempimenti, Gap analysis, Ipotesi di adeguamento, Formazione
 - Tempi:
 - impegno: da 20 a 50 gg/uomo
 - calendario: da 2 a 120 giorni
 - Forti problematiche organizzative

- **28 IT General Control**
- Supporto alla certificazione di bilancio
- PMI, Finanziarie
 - Verifica affidabilità Sistemi Informativi
 - Tempi:
 - impegno: da 2 a 3 gg/uomo
 - calendario: da 2 a 5 giorni
 - Poco tempo, intervento mirato

- **Sicurezza delle informazioni**
- **1BS7799, 4 ISO27001, 2 Assessment (CobIT), 2 Risk A&M, 1 Incident Mngmt, 53 PdSA, 1 Log Analysis, 1 linee guida per e-government, 2 I&AM**
- **Aziende Finanziarie, Telecomunicazioni, Centri Servizi, Trasporti, PAC, PMI**
 - Consulenza alla certificazione, redazione documentale e procedurale, Gap analysis.
 - Tempi:
 - impegno: da 20 a 200 gg/uomo
 - calendario: da 20 a 120 giorni

- **2 Assessment ITIL, v.2**
- Aziende Finanziarie, Telecomunicazioni,
 - Verifica processi, redazione documentale e procedurale, Gap analysis.
 - Tempi:
 - impegno: da 20 a 200 gg/uomo
 - calendario: da 20 a 120 giorni

- **1 Verifica Sarbanes Oaxley Act**
- Sezione 404
- Azienda Finanziaria
 - Verifica processi, redazione documentale e procedurale, Gap analysis su 29 applicazioni
 - Tempi:
 - impegno: 300 gg/uomo
 - calendario: 90 giorni

- **Progettazione e redazione corsi di sicurezza delle informazioni**
- P.A.C
 - 76 ore, 1520 slide
 - Tempi:
 - impegno: 120 gg/uomo
 - calendario: 90 giorni

- **Progettazione nuovo sistema informativo**
- P.A.C
 - Tempi:
 - impegno: 270 gg/uomo
 - Calendario: 270 giorni

- Tempi ristretti
- Costi molto contenuti
- Buona (alta...) qualità
- Poco invasivo
- Realizzabile
- Adatto alla situazione/azienda specifica
- Generalizzabile / in linea con il settore di mercato
- ...

- **FINANZA: conservativo**
 - 24x7 Business Critical, quasi Mission Critical
- **TELCO: tecnologico**
 - 24x7 Mission Critical
- **GOVERNO: paziente**
 - 24x7 ideale per i cittadini, 20x6 sufficiente
- **GRANDI IMPRESE: pianificazione**
 - B2B Business Critical, 23x7?
- **MEDIA, T&T, Utilities: il Mercato decide**
 - 24x7 Business Critical, Mission Critical
- **PMI: prudenti**
 - 23x7 va bene
- **SOHO: è presto...**

No One Size Fits All

No Silver Bullet

- Leggi specifiche: ad esempio Basilea II, controlli ABI, BI, oppure ISVAP e ANIA, CONSOB.
- Qualche certificazione ISO27001 su base volontaria (5 delle 52 in Italia)
- Qualche SOX, perchè acquisite da Banche o Assicurazioni straniere
- Qualche ITIL, perchè acquisite da Banche o Assicurazioni straniere
- Qualche CobiT, nei confronti dei Centri Servizi che forniscono i servizi in Outsourcing
- Conformità alla Privacy: DPS aggiornato
- Business Continuity: lavori in corso
- Molti IT internal Audit nelle organizzazioni più grandi

- Missione: la gestione del rischio
- Atteggiamento conservativo
- Budget IT: medio buono
- L'auditor, il verificatore è visto come un intruso, che non sa e vuole parlare di cose che non conosce abbastanza
- Forte attenzione ai processi interni
- Nei confronti dei clienti, vengono ritenute più importanti le ragioni del marketing che l'attenzione ai rischi tecnologici
- Importantissimo conoscere bene il settore:
 - Banche, ABI, Banca d'Italia, norme, ecc.
- Capire come muoversi con prudenza

- Norme specifiche: ETSI, ITU-T,
- Varie certificazione ISO27001 su base volontaria (9 delle 52 in Italia)
- Diffuso utilizzo di ITIL, perchè la gestione della tecnologia ICT deve essere di altissimo livello
- Conformità alla Privacy: DPS aggiornato, gestione delle intercettazioni
- Business Continuity: mission critical
- IT internal Audit e Risk Management

- Missione: la gestione delle comunicazioni 24 su 24 ore
- Atteggiamento tecnologico, innovativo, attento al mercato
- Budget ICT: alto-altissimo
- L'auditor, il verificatore è visto quasi come un collega
- Forte attenzione ai processi cliente: fatturazione.
- Nei confronti dei clienti, a volte il marketing anticipa la tecnologia
- Importante conoscere bene i servizi
- Capire come muoversi con competenza

- Norme specifiche per ogni mercato / settore
- Varie certificazione ISO27001 su base volontaria (12 delle 52 in Italia)
- Diffuso utilizzo di ITIL, perchè la gestione della tecnologia ICT deve essere di altissimo livello
- Conformità alla Privacy: DPS aggiornato, anche per i loro clienti
- Business Continuity: mission critical
- IT internal Audit e Risk Management
- CobiT per gli SLA

- Missione: il servizio al mercato, 24 su 24 ore
- Atteggiamento tecnologico, innovativo, attento al mercato
- Budget ICT: alto
- L'auditor, il verificatore è visto quasi come un collega
- Forte attenzione ai processi cliente: fatturazione.
- Ogni settore ha le sue peculiarità
- Importante conoscere bene i servizi
- Capire come muoversi con competenza

- Norme specifiche: Codice della Amministrazione Digitale (82/2005 e s.m.i.), libro Blu del CNIPA, ecc.
- E-governement, Cooperazione applicativa, PEC, CIE, CNS, FD.
- Una certificazione ISO2700: Comune di Segrate
- Richiesta di conformità UE per un caso, contributi per l'agricoltura
- Scarso utilizzo di ITIL, tranne casi particolari: Entrate e Difesa
- Conformità alla Privacy: DPS non aggiornato
- Business continuity: cos'è?
- Consapevolezza IT generalmente scarsa.

- Missione: servizi ai cittadini
- Atteggiamento iperprotettivo, i dati sono miei (e guai a chi me li tocca)
- Budget ICT: medio
- L'auditor, il verificatore è visto come un intruso
- I processi sono ingessati dalla burocrazia
- A volte sono così specifici da risultare di fatto unici
- Capire come muoversi con prudenza per accreditarsi

- Norme specifiche: CEN TC251, UNI U72, ISO TC215, ANSI-HL7, ANSI IEEE, ANSI-ASTM
- DPS, Privacy e dati sensibili: argomento molto delicato
- No certificazioni ISO27001.
- Scarso utilizzo di ITIL, tranne casi particolari
- Business Continuity: se c'è il pronto soccorso...
- Consapevolezza IT generalmente scarsa

- Missione: servizi ai cittadini, salvare la vita
- Molta attenzione da parte dei direttori delle UOC (primari)
- Tecnologia medica sempre più presente
- Amministrativi meno innovativi
- Budget IT: medio
- L'auditor, il verificatore è visto come uno che aggiunge problemi
- Il passaggio al digitale è appena iniziato: la cartella unica è un obiettivo futuro.
- Capire come muoversi e non stupirsi (Le piscine)

- Norme specifiche per settore
- Qualche certificazione ISO27001 su base volontaria (18 delle 52 in Italia)
- Qualche SOX, perchè acquisite da Aziende straniere
- Qualche ITIL, perchè acquisite da Aziende straniere
- Conformità alla Privacy: DPS abbastanza aggiornato
- Business Continuity: a seguito della produzione
- IT internal Audit nelle organizzazioni più grandi
- C'è di tutto...

- Missione: produrre utili, per gli stakeholder
- Atteggiamento vario (a volte la IT è considerata un male necessario, come le pulizie e la mensa, figurarsi il controllo sull'IT)
- Budget IT: dipende, da 0,1 % a 5% del fatturato
- L'auditor, il verificatore è visto inizialmente come un intruso, ma si riesce facilmente ad ottenere la fiducia degli interlocutori
- Forte attenzione ai processi di produzione e vendita
- Utile conoscere bene il settore specifico
- Capire come muoversi con competenza

Azienda	Settore	Utenti	Struttura IT	Server	Rating
1- <u>SiI</u>	Lavorazioni meccaniche	30	1	2	3
2- GDB	Produzione meccanica	600	15	10	8
3 - GSB	Produzione meccanica	200	4	8	6
4 - TI	Produzione meccanica	200	4	8	6
5 - SAE	Produzione meccanica	300	10	20	9
6 - PM	Produzione meccanica	200	3	1	7
7 - SFS	Produzione meccanica	130	1	9	6
8 - PW	Produzione elettromeccanica	160	4	16	7
9 - MA	Rivenditore macchine	50	4	13	5
10 - CO	Produzione meccanica	400	8	8	5
11 - GA	Lavorazioni meccaniche	40	1	2	5
12- IT	Produzione meccaniche	150	6	6	5
13 - VC	Rivenditore macchine	61	4	12	6

- **ISO27001:2005 (ex BS7799)**
 - 11 Domini, 133 controlli
 - Diffusione scarsa (52 in Italia)
 - Obbligo assente fino ad oggi in Italia,
 - Un caso UE per Organismi Pagatori in Agricoltura
 - Verticale, di processo, molto utile
 - Impegnativo
 - Consulenza, conformità, adeguamento, certificazione

- **D.Lgs 196/03, Privacy**
- Allegato B, Misure Minime
- Si basa sulla ISO27001
 - 29 Controlli
 - Obbligo presente in Italia, ma sottostimato
 - Come le cinture di sicurezza e il casco in moto
 - Consulenza, conformità, adeguamento, formazione

- **CobIT 4.1 (era 3.0)**
- IT Governance
 - 4 aree
 - 34 Domini, 360 controlli
 - Diffusione scarsa
 - Obbligo assente fino ad oggi in Italia
 - Un caso UE per Organismi Pagatori in Agricoltura
 - Molto completo, di processo
 - Impegnativo, da ritagliare per adattarsi a obiettivi
 - Consulenza, verifica

- **ITIL v.2 Gestione Sistemi Informativi**
 - 11 Domini
 - Verticale, pragmatico
 - Diffusione buona nei Data Center
 - Non troppo impegnativo, da ritagliare a piacere
 - Consulenza, verifica
- **ITIL v.3 Il Ciclo di Vita del Servizio Sistemi Informativi**
 - 23 Domini
 - Più ampio, meno pragmatico
 - Apena uscito
 - Sembra impegnativo, da ritagliare opportunamente
 - Consulenza, verifica

- Sarbanes Oxley Act
- BS25999 Business Continuity
- ISO20000
- 231
- 262
- ...

- **Prima**
 - Prepararsi
 - Conoscere il mercato di riferimento
 - Conoscere l'azienda, navigare sul sito web
 - Sentire i colleghi
- **Durante**
 - Chiedere con gentilezza
 - Cercare di capire, coinvolgere
 - Dare qualche consiglio, aiutare
- **Dopo**
 - Verificare, riflettere
 - Ringraziare

- **Durante**
 - Insistere
 - Pensare di aver capito tutto
 - Offendersi se non si ottiene risposta
 - Stupirsi troppo
 - Fare “l'ispettore”
- **Dopo**
 - Presentare male i risultati

- Da noi non è mai successo
- Se le dessi un milione di Euro , mi farebbe dare un'occhiata alla sua password?
- Se mi chiede questo, me ne vado
- Non ne posso più, è il terzo (quarto, quinto) audit in un mese!
- Bello questo disegno di rete, te lo rimando aggiornato

Cosa si può fare

- In 2-3 giorni:
- Fotografia dei SI, o preparazione per un progetto
- Se c'è grande collaborazione da parte del cliente

- In 20-50 giorni:
- Assessment, conformità, Gap Analysis, Risk Analysis, BIA
- Solo per servizi verticali, per settori o per aziende medio piccole
- Se c'è grande collaborazione da parte del cliente e supporto dalla direzione

- In 200-600 giorni:
- Assessment, conformità, Gap Analysis, Risk Analysis, BIA, progetti specifici, ecc.
- Processo completo, per settori o anche per aziende di rilevante dimensione
- Se c'è grande collaborazione da parte del cliente e supporto dalla direzione

- **Allineamento strategico**
- **Produzione del valore**
- **Gestione del rischio**
- **Gestione delle risorse**
- **Misura delle prestazioni**



N	Area	Norme di riferimento	Domanda	Scala	Peso
1	Allineamento strategico	CobiT 4.1 COSO	Quante leggi specifiche, associazioni, standard?	10: 3	3
2	Produzione del valore	CobiT 4.1 COSO		8: 2,5 6: 2 4: 1,5 2: 1 1: 0,5	
3	Gestione del rischio	ISO27001:2005	DPS? (Misure Minime)	Ottimizzate: 3 Operative: 2,5 Iniziate: 2 Definite: 1,5 Considerate: 1 Inesistenti: 0,5 Ignose: 0	3
4	Gestione delle risorse	ITIL BS25999	Se stacco questo cavo in sala macchine, cosa succede? Risposta entro: (Quali servizi non sono più raggiungibili, quali utenti non possono più eseguire le loro mansioni, qual'è l'impatto per l'azienda.)	10 minuti: 4	4
5	Misura delle prestazioni			20 minuti: 3,5 30 minuti: 3 45 minuti: 2,5 60 minuti: 2 2 ore: 1,5 4 ore: 1 8 ore: 0,5	
TOTALE					10

**Grazie, zio
Albert!**

prampolini@ordine.ingegneri.vi.it

