GRC – Preliminar Assessment

Sopralluogo presso	: **RS & Management Srl**
Sito operativo	: Vicolo delle Siepi 2
Sede Legale	: **00072 Ariccia (RM)**
Attività	: **Prodotti Informatici di Management aziendale**
Referente	: **Dott.ssa Sara Borelli**
Presenti alla intervista	: **Soci e partners tecnologici richiesti: SEFT Srl**
Richiesta consulenza	: **Integrazione regolatoria, adempimenti e adeguamenti ICT di settore**
Normative applicabili	: **Data Protection, Data Retention, IT Security, IT Governance, CC SaaS**
Prescrizioni legge	**: Dlg.196/03, Dlg.231/01, Dlg.81/10 (migrazione GDPR/EU /Reg.679/16)**
Allegati	: **comunicazioni elettroniche intercorse, Matrice audit, Questionario**

Contatto preliminare: 03/03/2016

Prescrizioni Legali, normazioni e Regolamenti applicabili all'ambito

TUS - Testo unico sulla sicurezza Telematica - ISO/IEC 9594-8:2014; Agid - misure fissate dal Garante provv.doc. web n. 4129029, Gazzetta Ufficiale n. 179 del 4 agosto 2015
Agenda Digitale e Protocollo Informatico PPAA - Decreto legge 22 giugno 2012, n. 83 e Circ. 2/2017 CAD emend. Dic 2017
Data Retention e Data Protection - Conservazione e Copie di Sicurezza Repertori Informatici; Accountability, LOG policy, DPO
Trattamento dei Dati Personali - Sistema Privacy Dlg.196/03, Dir. 95/46/EU, GDPR-UE : Amministratori di Sistema, Titolari del Trattamento, Responsabili del Trattamento, DBA, DPO.
Sicurezza delle Infrastrutture - Schemi di riferimento ISO27001 (data center e CED); ISO2000 (servizi IT), BC/DR
Sicurezza delle Reti e Readiness Perimentrale : IDS/IDP, OWASP, Data Breach Directive, NIST IH/IR, I-Team
Migrazione CLOUD Computing - CCSK Compliance, CSA: ENISA - Protocols & Procedure for Hypervisors System Managers

Linee Guida DBA e ADS e Basi giuridiche di Settore

- UNI ISO 15489-1 UNI ISO 15489-2: 2007: 2006 Informazione e documentazione - Gestione dei documenti di archivio Principi generali sul record management.
- CNDCEC – FNC – Gruppo di Lavoro del Consiglio e Fondazione Nazionale Commercialisti e Contabili 4/2018 – CheckLista GDPR.
- ISO/TS 23081-1:2006 Information and documentation - Records management processes – Metadata for records – Part 1 – Principles, Quadro di riferimento per lo sviluppo di un sistema di metadati di gestione .
- ISO/TS 23081-2:2007 Information and documentation - Records management processes – Metadata for records – Part 2 – Conceptual and implementation issues, Guida pratica per l'implementazione.
- ISO 15836:2003 Information and documentation - The Core metadata element set, Sistema di metadata

Dott. Salvo Reina
GRC & DP senior advisor

Tel.: +39 [010] 8685187
Cell.: +39 348 8528607
e-mail: dpo@salvoreina.it

Data : **10/03/2016**

Auditee : .....

Sopralluogo Pre-Audit : 10/03/2016

PREMESSA E BRIEFING DI INIZIO

La intervista ricognitiva preliminare non implica sopralluogo degli ambienti produttivi e/o delle aree ICT; questa prima occasione di raccolta conoscitiva ha lo scopo di acquisire dalla Proprietà, solamente gli elementi fisici, logici e organizzativi funzionali ad una indagine GRC (*Governance Risk & Compliance*). Gli indicatori sostanziali derivati indicheranno la postura aziendale nei confronti dei requisiti e degli adempimenti sugli schemi indicati in frontespizio del presente documento.
La pianificazione di futuri interventi di progettazioni di un aggiornamento tecnologico, normativo e procedurale sistemici orientati alla riorganizzazione della Sicurezza Informatica e Qualitativa del Sistema Aziendale, sarà vincolato a successivi mandati da parte della società Cliente.

AREE DI LAVORO	Data Center ☒	Uffici Amm. ☒	Sito freddo ☐
AMBITO DI AUDIT	Prima Parte ☐	Seconda Parte ☐	Terza Parte ☐
NORMAZIONI RIF	GDPR (priv.) ☒	ISO27001:u.r. ☐	ISO20000:u.r. ☐
	ITIL library ☐	CoBIT (GRC) ☐	ISO22301(BMI) ☐

OGGETTO APPLICABILE DI AUDIT (*marcare solo check-list applicabili*)

☒ Ricognizione e consultivazione Asseta SI, procedure, check-list (*vedi GRC-Preliminar Interview: Pag.3*)

☐ Scanzione check-list degli elementi di business, criticalità di processo e ambiti di valutazione per successive fasi di studio (*vedi modulo Business GAP analysis: Pag.4*)

☒ Acquisizione evidenze ***Skip-lot*** (supporti esterni, copie VM), copie sistematiche documentali, Patch management, Licences review and listing. (*vedi ANNESSO*)

CRITERI CONVENUTI (*marcare solo check-list applicabili*)

1. Eventuali acquisizioni di reperti documentali, e/o digitali sotto qualunque formato e supporto, sono collezionati e classificati alla presenta del Soggetto di Audit (Liceità di consenso presso interessato)
2. Le normazioni Q/S applicate all'oggetto di audit non sono considerate cogenti quindi usate come linee guida di riferimento per la indagine conoscitiva (Art. 13 Reg.679/2016)
3. Eventuali Annessi sono parte integrante della conduzione congiunta della intervista e saranno inclusi nella relazione di audit solo se controfirmati dall' Auditor e dal Soggetto di Audit

Ora locale di inizio : 9:30 Ora locale di fine : 11:20

Auditor

Dott. Salvo Reina
CISA, LA-ISO27001, LA-ISO20000
ISACA, BSI, CCP, CCSK-CSA

.....

Soggetto di Audit

.....
per
la Azienda

.....

GRC – Preliminar Interview

❑ **1.0 Verifiche preliminari stato corrente :**

1.1 **Assetto formale prescrittorio** : Censire e classificare tutti i documenti in essere come Sistema Documentale per il Trattamento dei Dati Personali ai sensi dei correnti termini di legge e accordi vincolanti di settore; profilazione o dati Extra UE?

1.2 **Acquisire copia di documenti** relativi alla conduzione della Gestione SI : mansionari, passaggi di consegna, elenchi e check-list procedure, evidenze di Asset Management. Deleghe e nomine

NO: ADS 2 Server + 4 VM – VMware [illegible]

❑ **1.2. Assetto formale volontario** : Sono in essere uno o più Sistemi di Qualità in accordo ad un riconosciuto schema certificazione e/o di accreditamento di Settore? (Es : ISO14001/EMAS, OHSAS /ISO 18000, ISO9001, ISO31000 ecc).

No ISO 27001/2000

❑ **1.3. Accountability Segregazione delle Responsabilità** : sono disponibili mappe di attribuzione di Gestione dei servizi e corrispondenti Deleghe di attribuzione per le figure di ADS e DPO? ES: Quali sistemi di autenticazione dall'esterno sono disponibili? (es. VPN, FTP, Ecc.) Appalti PP.AA.?

1 VPN / LOG / FTP - NO SSH/TLS 1.2

❑ **1.4. Piano di audit per data protection distribuito** –disponibilità di verifica dei LOG ? (Per quanto tempo e come sono conservati i file di log dei server, Es :mail server?) Verifica frequenza dei backup Email System? Riqualificazione fornitori esterni e contratti manutenzione. Documento di Valutazione dei Rischi? Es : DVR con CCP della superficie di attacco. IDS/IPS

CARTACEO → Prodotto e [illegible] → [illegible]

❑ **1.5. Migrazione CC di DP & Sistema Privacy Dlg.196/03** : disciplinare interno ICT, nomine ADS e DPO, adempimenti Data Breach, Periodo di conservazione dei Log di Sistema/Servizi/Applicazioni; utilizzo Servizi Cloud; Registro Trattamenti; banche dati intramurali (ano-pseudonimizzazione)

SQL Server 2008 Ent. | SEGMENTAZIONE VLAN

❑ **2.0 Sicurezza Perimetrale** : misure fisiche, logiche e organizzative DHCP/DMZ/sezionamenti/LDAP/AD. Es Gestione Autenticazioni e autorizzazioni. Artt. 34, 38 Dlg.196/03? Layout accesso data center (serramenti, lock-digitali, biometria?); BC/DR UPS/ tamp. Gruppo E. MDM o Rilevamento presenze (Dati dipendenti); CRM e fornitori Dichiarazioni transattive, BCR, Accordi di settore,

NO STATIC / PARZIALE / NO MDM /

GDPR COMPLIANCE – requisiti di migrazione di SPD

☐ 1.0 in atto o pianificato il processo di **identificazione delle tipologie di dati trattati**, delle finalità, dei differenti trattamenti operati e degli obiettivi perseguiti da ogni singolo trattamento?

.....NO.....

☐ 1.2. in atto o pianificata la **redazione del mansionario Privacy** atto a definire l'organigramma con ruoli e competenze interne ed esterne all'organizzazione aziendale, nell'ambito della gestione dei dati personali?

.....

☐ 1.3. in atto o pianificato l'aggiornamento delle lettere di **nomina ai soggetti interni** intervenenti nel trattamento dei dati (dipendenti e **soggetti terzi**) con l'adeguamento e l'assimilazione delle variazioni intervenute con l'emanazione del c.d. "**Job Acts**"?

.....

☐ 1.4. in atto o pianificata redazione del **Disciplinare tecnico** ad uso del personale interno e contestualmente l'aggiornamento delle varie **informative da rendere a dipendenti, clienti, fornitori, ecc.** con specifica attenzione ai dati che potrebbero essere trasferiti verso **paesi "terzi"** non facenti parte della EU, dei processi per l'**esercizio dei diritti dell'interessato** e delle formule di **consenso al trattamento**?

.....ROMANIA.....

☐ 1.5. in atto o pianificata la individuazione e **contrattualizzazione delle deleghe privacy** ai oggetti esterni all'organizzazione del titolare (redazione della contrattualistica riguardante gli incarichi di Responsabile/i esterni del trattamento e, ove da nominarsi, dei sub-Responsabili, ecc.) con la stesura del **disciplinare interno** relativo al trattamento dei dati personali ad uso del personale facente parte dell'organizzazione del titolare

.....

☐ 1.6. in atto o pianificata la **verifica dell'architettura di sicurezza**, e la armonizzazione di misure di sicurezza adeguate alle architetture informatica o in corso di implementazione oltre la verifica delle procedure dei **sistemi di autenticazione ed autorizzazione**, di gestione delle passwords e/o dei sistemi di rafforzamento delle autenticazioni degli **utenti nomadici**?

.....

☐ 1.7. in atto o pianificato **aggiornamento delle procedure RAEE** (rifiuti di elettrici ed elettronici) con valutazione rispondenza al provvedimento emanato dall'Autorità Garante oltre a verifica **sicurezza fisica** adottata per l'accesso **archivi cartacei/informatica** e anche la verifica delle procedure per la gestione e **custodia dei documenti cartacei** contenenti dati personali formalizzando redazione delle **privacy policy del sito internet**?

.....

☐ 1.8. in atto o pianificata **redazione delle informative del sito internet** e di quelle specifiche per particolari categorie di interessati insieme a redazione informative semplificate sui cookies oltre **valutazione ed analisi dei rischi, degli impatti negativi** su libertà ed i diritti degli interessati, formalizzando **misure tecniche e organizzative** adottate e da adottare per mitigarli?

.....

☐ 1.9. in atto o pianificato supporto nella **valutazione della rispondenza di conformità** dei trattamenti operati in base ai principi cardine del GDPR di "***privacy by design***" e "***privacy by default***" oltre alla assistenza annua in termini di consulenza per mantenere costantemente aggiornato il cliente sulle mutazioni in tema di trattamento dei dati personali, che lo riguardano in maniera diretta?

INDAGINE CONOSCITIVA – GAP Analysis

PROCESSO DI BUSINESS VERSUS RIORGANIZZAZIONE ITC SECURITY

Le norme e gli schemi di riferimento sono adottati in quanto linee guida quindi i punti sono marcati anche se non applicabili ed in questo caso le voci interessate sono commentate per iscritto (o tramite trascrizione di clip audio) con la notazione (N.A.) I punti sono investigati secondo criteri di pertinenza e finalità arbitrariamente scelti dall'auditor. Prima di rispondere il Soggetto di Audit può chiedere lo stralcio da eventuali registrazioni audio. Nel caso di non risposta le caselle rimangono inalterate. Deroghe o varianti alla compilazione sono annotate nell' Annesso B

VERIFICHE PROPEDEUTICHE ALL'INCONTRO ED ELEMENTI DI *E-DISCOVERY*

Scadenze Certificati Iso9001 (clausole 1-3 conformità a prescrizioni legali), portale back-office accesso credenziali (landing page senza informativa); raccolta dati interessato a mezzo preventivazione on-line; consenso inidoneo non informato e pre-flaggato; cartiglio senza termini di trattamento e/o informativa. Certificazione / base giuridica di settore (Direttiva RoHS). Contrattualistica per assistenza tecnica e collaudi RDT externo; dichiarazioni di conformità e attestati di collaudo sub-committenze

ORGANIZATION	HARDWARE
☐ IT Organization chart and client structure (quantity, type, location) ☐ Employee list (name, responsibility, start date) ☐ Support-desk approach and change-management process	☐ CPUs and location ☐ Databases (numbers, brands & types) ☐ Networks by location (LAN/WAN) ☐ Telecommunications/connectivity approach
SYSTEMS SOFTWARE	**APPLICATIONS SOFTWARE**
☒ Operating systems ☒ Application systems development software ☐ Database management systems ☐ Security ☐ Current technology? ☐ Life expectancy? ☐ Replacement/upgrade strategy?	☒ Application systems ☐ Developed in-house vs. third party ☐ Electronic interfaces ☒ Payer interfaces ☐ Standard across the network? ☐ Approach to release management ☐ Report-writing capability ☐ Support approach and known issues
EXISTING AND PLANNED PROJECTS	**OPERATING BUDGET AND P&L TRENDS**
☐ Large-scale projects (i.e., reengineering, new systems, SW development) ☐ Midrange enhancements ☐ Software support backlog ☒ New business development needs ☐ Productivity enhancements ☐ Payer requirements ☐ New technology R&D ☐ Consulting and/or contractors needs anticipated (next 12 months)	☐ Personnel ☐ Software maintenance ☐ Hardware maintenance ☐ Equipment leases and rental ☐ Supplies ☐ Data communications ☐ Voice communications ☐ Outside contractors ☐ Rent related to IT equipment and staff ☐ Postage ☐ Consulting/contractors
CAPITAL BUDGET	**CONTRACTS**
☐ Immediate needs (next six months) ☐ Anticipated need for normal growth (next 18 months)	☐ Software licenses ☐ Software support and maintenance ☐ Hardware leases ☐ Hardware maintenance ☐ Software and/or hardware purchase agreements (ownership) ☐ Contract programmers or other consulting agreements ☐ PC software licenses
COMPUTER OPERATIONS	
☐ Service level (response time, system availability, report distribution, etc.) ☒ Network management (circuit uptime, new installations, changes planned) ☐ Batch process	

memo post odg

email Corporate
INFORMATIVE WEB
Termini VSO

SECONDA FASE DI PRIORITA' - Assetto GAT

- *Progetto privacy - ex post Codice196 migrazione (RDT e Sub-RDT)*
- *formazione contestuale ad inizio progetto Insieme omine deleghe (INT/EXT)* (Revisione Contratti) elicenze
- *basi giuridiche immediate per DVR e DPIA (equiparabile Call Center)* → Profilazione operatori?
- *Affiancamento IT adeguamento LAN/Web con informative immediate!* → STATS ATTIVITA'?
- *Manuale SP via WEB: intralan Server IIS dedicato*
- *postazione li lavoro H24/7gg/365 (NUC) per inizio scanzioni LAB ai fini DVR*

SECONDA FASE DI PRIORITA' - Postura formale

- *Registro trattamenti* → entro 2 mesi: (2 settimane con SW PEVO)
- *DPIA - acquisti essenziali (NAS/NUC/pendrives minuteria disposable)*
- *Pentest e VA - Mattia Epifani intervento con RealityNet System Solution*
- *Politiche di difesa perimetrali: ACL share folders,* (Alert GLASSWIRE)

TERZA FASE DI PRIORITA'

- *Audit di verifica e controllo*
- *A regime: Log management/modifiche di sistema,*
- *DataBreach Incidente response team*
- *Sito freddo - Remote storage RSYNC*

SOSPESO FINO Co Titolarità

NOTE PER LA PROPRIETA' - CONTRATTO E INCARICO

Prima del PDI: ***retroattività documentale Piano di Adeguamento e Piano di formazione per designazione; retroattività misure minime e disciplinare (fatture di acquisti IT negli ultimi anni);***