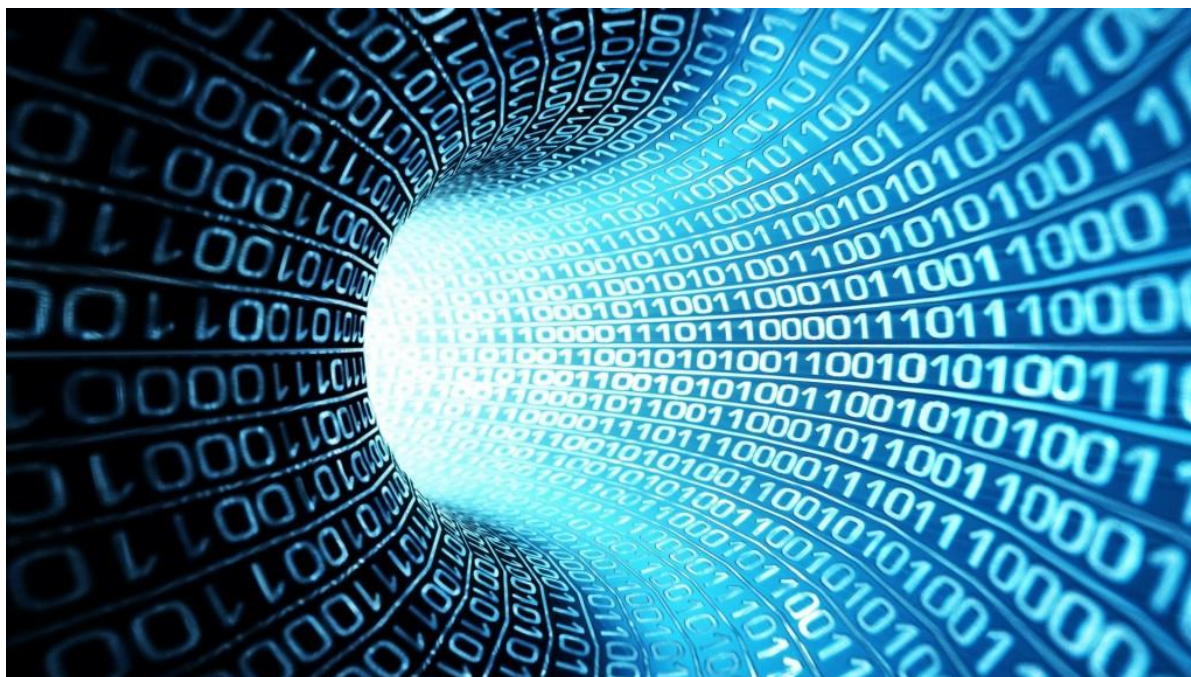


## Referenze di Progetto



Luglio 2020

## Indice Referenze

1.	Project Management .....	3
2.	Information Security Compliance (Area Privacy) .....	5
3.	Data Protection Officer e Supporto DPO Interni .....	8
4.	Compliance Internazionale .....	11
5.	Information System Audit Process.....	12
6.	Information Security Risk Analysis e Management .....	14
7.	Progettazione e supporto all'implementazione di SGSI ISO 27001– 27017 – 27018 .....	16
8.	Progettazione e supporto all'implementazione di SGQ ISO 9001 .....	19
9.	Progettazione e supporto all'implementazione di SGS ISO 20000 .....	22
10.	Security Assessment & Monitoring: Penetration test & Vulnerability Assessment .....	23
11.	Logical Security Controls System Configuration .....	23
12.	Logical Security Controls Account & User Management .....	24
13.	Incident Management.....	25
14.	Business Continuity Plan .....	26
15.	Security Awareness.....	28
16.	Modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001 .....	30
17.	IT Governance .....	31
18.	Data Integrity – Data Governance – Data Quality .....	32

## 1. Project Management

**Cliente:** Brandart Image Packaging Srl – Busto Arsizio

**Intervento:** Gestione del progetto riguardante l'implementazione del sistema applicativo a supporto del processo di gestione dei fornitori.

**Attività svolte:** Pianificazione delle attività progettuali, Analisi dei requisiti funzionali e di sistema, Monitoraggio dell'avanzamento delle attività, Gestione delle issues e dei problemi.

**Cliente:** Brandart Image Packaging Srl – Busto Arsizio

**Intervento:** Gestione dei progetti riguardanti l'implementazione di Applicativi Gestionali basati sulla suite SAP R/3 moduli FI, CO, MM, SD, PS.

**Attività svolte:** Pianificazione delle attività progettuali, Analisi dei requisiti funzionali e di sistema, Monitoraggio dell'avanzamento delle attività, Gestione delle issues e dei problemi.

**Cliente:** ACEA SpA – Roma

**Intervento:** Gestione dei progetti riguardanti l'implementazione di Applicativi per il Credit Management Area Customer Operation per i settori Idrico, Energia, Distribuzione.

**Attività svolte:** Pianificazione delle attività progettuali, Analisi dei requisiti funzionali e di sistema, Monitoraggio dell'avanzamento delle attività, Gestione delle issues e dei problemi.

**Cliente:** San Raffaele SpA – Roma

**Intervento:** Gestione del progetto per l'implementazione del Dossier Sanitario Elettronico.

**Attività svolte:** Pianificazione delle attività progettuali, Analisi dei requisiti funzionali e di sistema, Monitoraggio dell'avanzamento delle attività, Gestione delle issues e dei problemi, Formazione a beneficio degli utenti.

**Cliente:** Peroni SpA – Roma

**Intervento:** Progettazione di un processo di Data Cleaning a supporto dell'elaborazione dei dati di sell-out ed implementazione di un sistema di calcolo automatico della relativa reportistica.

**Attività svolte:** Pianificazione delle attività progettuali, Analisi dei requisiti funzionali, Progettazione del processo, Definizione delle procedure di gestione del processo, Progettazione della base dati, Monitoraggio dell'avanzamento delle attività, Gestione delle issues e dei problemi.

---

**Cliente:** Guess Service – Roma

**Intervento:** Gestione del progetto per l'implementazione di un sistema di Business Activity Monitoring.

**Attività svolte:** Pianificazione delle attività progettuali, Analisi dei requisiti funzionali e di sistema, Monitoraggio dell'avanzamento delle attività, Gestione delle issues e dei problemi, Formazione a beneficio degli utenti.

---

**Cliente:** Sidel Participations S.A.S. (Gruppo Tetra Laval) - Parma

**Intervento:** Programme e Project Management nell'area ICT

**Attività svolte:** Monitoraggio dei progetti in portfolio, stato avanzamento e gestione delle issues rilevanti dei progetti presenti nel programma, ruolo di PMO a supporto dei Project Manager della funzione IT della Società.

---

## 2. Information Security Compliance (Area Privacy)

**Cliente:** Telecom Italia SpA – Roma

**Intervento:** Analisi di compliance dei sistemi che trattano dati di traffico (DDT) che agiscono in deroga ai requisiti di retention richiesti dal Provvedimento del Garante per la Protezione dei Dati Personali del 17/01/2008 ed alle policy e linee guida aziendali

**Attività svolte:** Censimento dei sistemi DDT che agiscono in deroga ai requisiti di retention richiesti dal Garante, Identificazione delle policy di retention adottate e delle motivazioni delle deroghe, Valutazione del livello di conformità rispetto alle deroghe ammesse dai regolamenti aziendali e comunicate al Garante.

**Cliente:** Telecom Italia SpA – Roma

**Intervento:** Assessment del livello di resilienza e del livello di riservatezza dei sistemi IT che trattano contenuti SMS.

**Attività svolte:** Analisi della documentazione aziendale riguardante i processi di resilienza e di riservatezza dei sistemi che trattano SMS (policy, linee guida, procedure operative, documentazione tecnica, piani di sicurezza, report), Definizione di Check List di controlli sui processi in esame basate sui requisiti indicati nell'articolo 14 del D. Lgs 70/2012, sulle linee guida in materia di misure di sicurezza dell'ENISA (European Network and Information Agency) e sui regolamenti aziendali, Definizione del perimetro di sistemi da sottoporre ad analisi, Interviste ai referenti aziendali coinvolti nei processi in esame, Raccolta delle evidenze, Realizzazione dei report di Audit, Executive Summary, Supporto alla definizione dei piani di rientro e di miglioramento.

**Cliente:** Gruppo Megaholding - Trani

**Obiettivi:** Revisione del framework di privacy compliance (D.lgs. 196/2003) e del framework per l'adempimento al provvedimento del Garante per la Protezione dei Dati Personali relativo agli Amministratori di Sistema.

**Attività svolte:** Assessment sul livello di compliance alla normativa sulla privacy dei processi aziendali (nomine, informative, consenso, notificazione dei trattamenti, misure minime di sicurezza, videosorveglianza, fidelity card, cookie), della contrattualistica con terze parti, della documentazione esistente relativa agli Amministratori di Sistema (lettere di incarico, elenco, Job Description, etc.), Identificazione del gap, Interviste agli Owner dei processi di trattamento dei dati personali, Censimento dei trattamenti di dati personali, Redazione della documentazione per la compliance al provvedimento relativo agli Amministratori di Sistema (Procedure, Elenco degli Amministratori di Sistema, Piano e Check List di Audit, etc.).

**Cliente:** Telecom Italia SpA – Roma

**Intervento:** Assessment sul livello di compliance dei processi di Log Management ai Provvedimenti del Garante per la Protezione dei Dati Personali del 17/01/2008 (Dati di Traffico) e del 27/11/2008 (Amministratori di Sistema) ed alle policy ed ai regolamenti aziendali.

**Attività svolte:** Analisi della documentazione aziendale riguardante i processi di Log Management (policy, linee guida, procedure operative, documentazione tecnica, piani di sicurezza, report), Definizione di Check List di controlli sui processi in esame basate sui Provvedimenti del Garante per la Protezione dei Dati Personali del 17/01/2008 e del 27/11/2008 e sui regolamenti aziendali, Definizione del perimetro di sistemi da sottoporre

ad analisi, Interviste ai referenti aziendali coinvolti nei processi in esame, Raccolta delle evidenze, Realizzazione dei report di Audit, Executive Summary, Supporto alla definizione dei piani di rientro e di miglioramento.

**Cliente:** Fendi Srl - Roma

**Intervento:** Revisione del Documento Programmatico sulla Sicurezza (D.lgs. 196/2003) e del framework per l'adempimento al provvedimento del Garante per la Protezione dei Dati Personali relativo agli Amministratori di Sistema.

**Attività svolte:** Assessment sul livello di compliance del DPS, della contrattualistica con terze parti, della documentazione esistente relativa agli Amministratori di Sistema (lettere di incarico, elenco, Job Description, etc.), Identificazione del gap documentale, Interviste agli Owner dei processi di trattamento dei dati personali, Censimento dei trattamenti di dati personali, Risk Analysis, Pianificazione degli interventi formativi, Redazione della documentazione per la compliance al provvedimento relativo agli Amministratori di Sistema (Procedure, Elenco degli Amministratori di Sistema, Piano e Check List di Audit, etc.).

**Cliente:** Sorgenia SpA - Milano

**Intervento:** Realizzazione della documentazione necessaria per l'adempimento al provvedimento del Garante per la Privacy relativo agli Amministratori di Sistema.

**Attività svolte:** Identificazione dell'ambito di intervento, Redazione di una Procedura operativa per l'adempimento al Provvedimento del Garante, Redazione delle Job Description per ciascun profilo di Amministratore di Sistema, Redazione dell'Elenco degli Amministratori di Sistema, Formazione, Definizione dell'Audit Plan.

**Cliente:** San Raffaele SpA - Roma

**Intervento:** Realizzazione della documentazione necessaria per l'adempimento al provvedimento del Garante per la Privacy relativo agli Amministratori di Sistema.

**Attività svolte:** Identificazione dell'ambito di intervento, Redazione di una Procedura operativa per l'adempimento al Provvedimento del Garante, Redazione delle Job Description per ciascun profilo di Amministratore di Sistema, Redazione dell'Elenco degli Amministratori di Sistema, Formazione, Definizione dell'Audit Plan.

**Cliente:** Birra Peroni SpA - Roma

**Intervento:** Revisione della documentazione di sistema gestione Privacy (D.lgs. 196/2003).

**Attività svolte:** Revisione del processo e dell'organizzazione per la privacy, di policy e procedure in essere, della contrattualistica con i fornitori, verifica compliance con Provvedimenti emanati dal Garante applicabili al settore, ai requisiti minimi di sicurezza e Formazione.

#### Cliente: Gruppo SOL - Monza

**Intervento:** IT Assessment al GDPR per la controllante italiana e per le altre società controllate in territorio UE.

**Attività svolte:** Identificazione dei sistemi IT gestiti centralmente per le Società del Gruppo SOL dalla Direzione Sistemi Informativi, definizione della tipologia di dati personali trattati, dei tempi di conservazione e delle misure di sicurezza in essere e conseguente definizione delle misure di sicurezza IT suggerite da implementare per la compliance al GDPR, Assessment on-site presso tutte le Società del Gruppo SOL con sede nell'Unione Europea per l'identificazione dei sistemi IT gestiti autonomamente e delle misure di sicurezza in essere in ottica di compliance al GDPR. Realizzazione di report con le risultanze dell'assessment e le azioni di trattamento suggerite per la compliance al GDPR.

#### Clienti Vari

**Intervento:** Attività di assessment e/o compliance al Regolamento (UE) 2016/659 – General Data Protection Regulation – GDPR per diversi clienti privati (Gruppo Megaholding, Gruppo Scavolini, Gruppo Renco, Leitwind, Gruppo Porcarelli, Tolfa Care, G.I.Ma, ASSILT), clienti pubblici, pubblici utilities e terzo settore (MISE DGIAI - Direzione generale per gli incentivi alle imprese, AMGA Legnano Spa, Roma TPL, Cotral, UNICEF).

**Attività svolte:** Assessment sul livello di compliance al GDPR dei processi aziendali (nomine, informative, consenso, notificazione dei trattamenti, misure di sicurezza, videosorveglianza, fidelity card, cookie), della contrattualistica con terze parti, della documentazione esistente relativa agli Amministratori di Sistema (lettere di incarico, elenco, Job Description, etc.), Identificazione del gap, Interviste agli Owner dei processi di trattamento dei dati personali, Predisposizione del Registro delle attività di trattamento (Art. 30 del GDPR), Redazione delle procedure per la gestione del Registro, delle richieste di esercizio dei diritti degli interessati, per la notifica di violazioni di dati (data breach), privacy by design & by default, Revisione delle informative dei dipendenti, outsourcer e clienti e degli aspetti privacy della contrattualistica, Conduzione della Valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment – DPIA).

#### Clienti Vari

**Intervento:** Formazione del personale dipendente al Regolamento (UE) 2016/659 – General Data Protection Regulation – GDPR per diversi clienti (Gruppo Mega, Gruppo SOL, G.I.Ma, UNICEF)

**Attività svolte:** Predisposizione dei contenuti per la formazione sia in modalità e-learning mediante piattaforma online da noi sviluppata e implementata che in aula con test di verifica finale dell'apprendimento per tutti i dipendenti delle società clienti.

#### Clienti Vari

**Intervento:** Offerta di una suite applicativa in cloud per la gestione della privacy compliance in modalità SAAS (Software As Service) denominata "P4U", attività di consulenza e di training per l'utilizzo del software (Gruppo SOL, Gruppo Renco, La Molisana, ASSILT, Tolfa Care).

**Attività svolte:** Attività di supporto nel caricamento delle informazioni societarie sulla piattaforma, addestramento dei referenti aziendali interni per l'utilizzo dell'applicativo o alternativamente gestione e



aggiornamento dei dati per conto delle Società Clienti, attività di assistenza su eventuali malfunzionamenti, miglioramento continuo delle funzionalità offerte.

### 3. Data Protection Officer e Supporto DPO interni

#### Cliente: Gruppo Megaholding - Trani

**Intervento:** Assunzione incarico come Responsabile della Protezione dei Dati (RPD) anche detto DPO – Data Protection Officer.

**Attività svolte:** Svolgimento delle funzioni di DPO con compiti di informazione e consulenza al Titolare del trattamento in merito agli adempimenti previsti dal GDPR, attività di verifica sull'osservanza delle disposizioni del Regolamento, controllo sullo svolgimento della formazione e della sensibilizzazione del personale, attività di cooperazione e punto di contatto tra le Società e il Garante nei casi previsti dalla normativa.

#### Cliente: AP Commerciale Srl - Napoli

**Intervento:** Assunzione incarico come Responsabile della Protezione dei Dati (RPD) anche detto DPO – Data Protection Officer.

**Attività svolte:** Svolgimento delle funzioni di DPO con compiti di informazione e consulenza al Titolare del trattamento in merito agli adempimenti previsti dal GDPR, attività di verifica sull'osservanza delle disposizioni del Regolamento, controllo sullo svolgimento della formazione e della sensibilizzazione del personale, attività di cooperazione e punto di contatto tra le Società e il Garante nei casi previsti dalla normativa.

#### Cliente: Dental Franchising Srl (Network Vitaldent) - Milano

**Intervento:** Assunzione incarico come Responsabile della Protezione dei Dati (RPD) anche detto DPO – Data Protection Officer.

**Attività svolte:** Svolgimento delle funzioni di DPO con compiti di informazione e consulenza al Titolare del trattamento in merito agli adempimenti previsti dal GDPR, attività di verifica sull'osservanza delle disposizioni del Regolamento, controllo sullo svolgimento della formazione e della sensibilizzazione del personale, attività di cooperazione e punto di contatto tra le Società e il Garante nei casi previsti dalla normativa.

#### Cliente: Gruppo Scavolini - Montelabbate

**Intervento:** Assunzione incarico come Responsabile della Protezione dei Dati (RPD) anche detto DPO – Data Protection Officer.

**Attività svolte:** Svolgimento delle funzioni di DPO con compiti di informazione e consulenza al Titolare del trattamento in merito agli adempimenti previsti dal GDPR, attività di verifica sull'osservanza delle disposizioni del Regolamento, controllo sullo svolgimento della formazione e della sensibilizzazione del personale, attività di cooperazione e punto di contatto tra le Società e il Garante nei casi previsti dalla normativa.

#### Cliente: ASSILT - Roma

**Intervento:** Assunzione incarico come Responsabile della Protezione dei Dati (RPD) anche detto DPO – Data Protection Officer .



**Attività svolte:** Svolgimento delle funzioni di DPO con compiti di informazione e consulenza al Titolare del trattamento in merito agli adempimenti previsti dal GDPR, attività di verifica sull'osservanza delle disposizioni del Regolamento, controllo sullo svolgimento della formazione e della sensibilizzazione del personale, attività di cooperazione e punto di contatto tra le Società e il Garante nei casi previsti dalla normativa.

**Cliente:** Tolfa Care Srl (Residenza Quinta Stella) - Tolfa

**Intervento:** Assunzione incarico come Responsabile della Protezione dei Dati (RPD) anche detto DPO – Data Protection Officer .

**Attività svolte:** Svolgimento delle funzioni di DPO con compiti di informazione e consulenza al Titolare del trattamento in merito agli adempimenti previsti dal GDPR, attività di verifica sull'osservanza delle disposizioni del Regolamento, controllo sullo svolgimento della formazione e della sensibilizzazione del personale, attività di cooperazione e punto di contatto tra le Società e il Garante nei casi previsti dalla normativa.

**Cliente:** YoctoIT Srl - Milano

**Intervento:** Assunzione incarico come Responsabile della Protezione dei Dati (RPD) anche detto DPO – Data Protection Officer .

**Attività svolte:** Svolgimento delle funzioni di DPO con compiti di informazione e consulenza al Titolare del trattamento in merito agli adempimenti previsti dal GDPR, attività di verifica sull'osservanza delle disposizioni del Regolamento, controllo sullo svolgimento della formazione e della sensibilizzazione del personale, attività di cooperazione e punto di contatto tra la Società e il Garante nei casi previsti dalla normativa.

**Cliente:** Fin Sarda Spa - Cagliari

**Intervento:** Assunzione incarico come Responsabile della Protezione dei Dati (RPD) anche detto DPO – Data Protection Officer .

**Attività svolte:** Svolgimento delle funzioni di DPO con compiti di informazione e consulenza al Titolare del trattamento in merito agli adempimenti previsti dal GDPR, attività di verifica sull'osservanza delle disposizioni del Regolamento, controllo sullo svolgimento della formazione e della sensibilizzazione del personale, attività di cooperazione e punto di contatto tra la Società e il Garante nei casi previsti dalla normativa.

**Cliente:** Gruppo Renco - Pesaro

**Intervento:** Supporto al Responsabile della Protezione dei Dati (RPD) anche detto DPO – Data Protection Officer interno.

**Attività svolte:** Redazione di pareri relativi alla liceità dei trattamenti, supporto nella gestione delle richieste di esercizio dei diritti degli interessati ai sensi degli artt.15-22 del GDPR, attività di audit sulla conformità delle disposizioni del Regolamento, attività di della formazione e della sensibilizzazione del personale in modalità e-learning e in aula.

**Cliente:** La Molisana S.p.A. - Campobasso

**Intervento:** Supporto al Referente Privacy interno.

**Attività svolte:** Redazione di pareri relativi alla liceità dei trattamenti, supporto nella gestione delle richieste di esercizio dei diritti degli interessati ai sensi degli artt.15-22 del GDPR, attività di audit sulla conformità delle

disposizioni del Regolamento, attività di della formazione e della sensibilizzazione del personale in modalità e-learning e in aula.

**Cliente:** G.I.Ma. Spa – Ponte San Giovanni

**Intervento:** Supporto al Referente Privacy interno.

**Attività svolte:** Redazione di pareri relativi alla liceità dei trattamenti, supporto nella gestione delle richieste di esercizio dei diritti degli interessati ai sensi degli artt.15-22 del GDPR, attività di audit sulla conformità delle disposizioni del Regolamento, attività di della formazione e della sensibilizzazione del personale in modalità e-learning e in aula.

**Cliente:** Gruppo SOL - Monza

**Intervento:** Supporto al Responsabile della Protezione dei Dati (RPD) anche detto DPO – Data Protection Officer interno.

**Attività svolte:** Redazione di pareri relativi alla liceità dei trattamenti, supporto nella gestione delle richieste di esercizio dei diritti degli interessati ai sensi degli artt.15-22 del GDPR, attività di audit sulla conformità delle disposizioni del Regolamento, attività di della formazione e della sensibilizzazione del personale in modalità e-learning e in aula.

---

---

## 4. Compliance Internazionale

**Cliente:** Data Management SpA - Genova

**Intervento:** Supporto all'implementazione di un impianto documentale di policy e procedure IT per la compliance ai principi SAS 70 – SSAE 16.

**Attività svolte:** Analisi dei processi IT aziendali, Gap Analysis rispetto ai requisiti di compliance richiesti dal framework di controllo aziendale, Redazione delle Policy e Procedure IT, Tuning dell'impianto documentale e supporto all'adozione.

**Cliente:** HRGest SpA - Genova

**Intervento:** Revisione dei Sistemi Informativi aziendali secondo i principi SAS70 e gli elementi applicabili e pertinenti degli ISA (*"International Standard on Auditing"*) al fine del rilascio dei Report SAS70 - Type I e Report SAS70 – Type II.

**Attività svolte:** Definizione dei Control Objectives, identificazione dei keycontrols, Analisi della sicurezza del sistema informativo aziendale (Hardware, Software e Networking) sulla base dei framework di riferimento Cobit, Analisi dei documenti a supporto di policies, procedure e standard in vigore, Valutazione dell'adeguatezza della documentazione e del design dei controlli, Documentazione delle risultanze, Follow-up.

**Cliente:** HRGest SpA - Genova

**Intervento:** Verifica della conformità della Business Unit IT ai requisiti della Sarbanes-Oxley Act sulla base di una lista di IT General Control.

**Attività svolte:** Analisi, della sicurezza del sistema informativo aziendale (Hardware, Software e Networking) e dei relativi processi di gestione sulla base dei framework di riferimento ISO/IEC 27001 e Cobit, Individuazione delle principali aree di rischio, Documentazione delle risultanze, Follow-up.

---

## 5. Information System Audit Process

**Cliente:** Istituto Poligrafico Zecca dello Stato

**Intervento:** IT Assessment, Analisi dell'architettura informatica ed individuazione delle azioni di mitigazione dei rischi IT.

**Attività svolte:** Analisi dell'impianto di Policy e Procedure, dei processi di sicurezza delle Informazioni, dei rischi e delle misure di sicurezza relativi al patrimonio informativo aziendale in termini di Persone, Informazioni, Processi, Infrastrutture hardware e di networking, Applicativi, Interviste a risorse coinvolte nei processi di sicurezza delle informazioni, Raccolta delle evidenze sul campo, Redazione del Report di Audit, Formalizzazione dei Rischi IT rilevati e delle Osservazioni, Monitoraggio dell'attuazione delle Remediation e delle Azioni di Miglioramento stabilite.

**Cliente:** Società di Certificazione internazionale: DNV GL

**Intervento:** Esecuzione di Audit di Terza Parte finalizzati al rilascio della certificazione ISO 27001 presso le seguenti Società: Telecom Italia, ACI Informatica, Accenture HR, Almaviva, Lottomatica, Aspasiel.

**Attività svolte:** Analisi dell'impianto di Policy e Procedure, dei processi di sicurezza delle Informazioni, dei rischi e delle misure di sicurezza relativi al patrimonio informativo aziendale in termini di Persone, Informazioni, Processi, Infrastrutture hardware e di networking, Applicativi, Interviste a risorse coinvolte nei processi di sicurezza delle informazioni, Raccolta delle evidenze sul campo, Redazione del Report di Audit, Formalizzazione delle Non Conformità, delle Raccomandazioni e delle Osservazioni, Monitoraggio dell'attuazione delle Azioni Correttive e Preventive stabilite.

**Cliente:** Società di revisione contabile e certificazione di bilancio – BDO Italia SpA

**Intervento:** IT Assessment, Analisi dell'architettura informatica ed individuazione delle azioni di mitigazione dei rischi IT per Società Clienti di BDO, tra cui: Megamark, Amet, Cosvim Energia, Acquedotto Lucano, Acquedotto Pugliese, IPA Sud, Magnaghi, Salver, Findast – Chimica D'Agostino, Pastificio Riscossa, Marseglia Group, Gruppo Matarrese, Gruppo SOL, Sixty Group, Gefran, HrGest, TotoCarovigno, Banca Popolare Valle d'Istria e Magna Grecia, ASL Basilicata, Ciccolella.

**Attività svolte:** Analisi, della sicurezza del sistema informativo aziendale (Hardware, Software e Networking) sulla base dei framework di riferimento ISO/IEC 27001 e Cobit, Individuazione delle principali aree di rischio, Identificazione delle relative azioni correttive per la loro mitigazione, Verifica dei processi informatici finalizzati alla definizione di poste di Bilancio, Presentazione delle risultanze al Management della Società ed all'Audit Committee.

**Cliente:** Società di revisione contabile e certificazione di bilancio – Ernst & Young

**Intervento:** IT Assessment, Analisi dell'architettura informatica ed individuazione delle azioni di mitigazione dei rischi IT per Società Clienti.

**Attività svolte:** Analisi, della sicurezza del sistema informativo aziendale (Hardware, Software e Networking) sulla base dei framework di riferimento ISO/IEC 27001 e Cobit, Individuazione delle principali aree di rischio, Identificazione delle relative azioni correttive per la loro mitigazione, Verifica dei processi informatici finalizzati alla definizione di poste di Bilancio, Presentazione delle risultanze al Management della Società ed all'Audit Committee

**Cliente:** Sorgenia SpA - Milano

**Intervento:** Analisi dell'architettura informatica ed individuazione delle azioni di mitigazione dei rischi.

**Attività svolte:** Analisi, della sicurezza del sistema informativo aziendale (Hardware, Software e Networking) sulla base dei framework di riferimento ISO/IEC 27001 e Cobit, Individuazione delle principali aree di rischio, Identificazione delle relative azioni correttive per la loro mitigazione, Presentazione delle risultanze al Management della Società e all'Audit Committee.

**Cliente:** Poste Italiane SpA - Roma

**Intervento:** Audit di prima parte relativo alla norma ISO 27001:2005.

**Attività svolte:** Verifica dell'impianto documentale a supporto del SGSI (Politica per la Sicurezza delle Informazioni, Campo di Applicazione, Analisi e Piano di Trattamento del Rischio, Dichiarazione di Applicabilità, Procedure Documentate, Procedure Operative, Registre del SGSI), Verifica della conformità dei processi in ambito SGSI rispetto ai controlli dell'Annex A ed ai punti della norma ISO/IEC 27001:2005, Rilevazione di non conformità e aree di miglioramento.

**Cliente:** Banca Intesa (Casse del Centro – Spoleto)

**Intervento:** Analisi dell'architettura informatica ed individuazione delle azioni di mitigazione dei rischi.

**Attività svolte:** Analisi, della sicurezza del sistema informativo aziendale (Hardware, Software e Networking) sulla base dei framework di riferimento ISO/IEC 27001 e Cobit, Individuazione delle principali aree di rischio, Identificazione delle relative azioni correttive per la loro mitigazione, Presentazione delle risultanze al Management della Società e all'Audit Committee.

## 6. Information Security Risk Analysis e Management

**Cliente:** Capgemini Italia SpA - Roma

**Intervento:** Analisi dei Rischi IT e Piano di Trattamento dei Rischi nell'ambito del processo di implementazione di un SGSI ISO/IEC 27001 compliant.

**Attività svolte:** Censimento e classificazione degli Asset IT, Definizione dei livelli di impatto sul business, Identificazione delle minacce al patrimonio informativo e delle vulnerabilità degli Asset IT, Valutazione dei livelli di rischio, Identificazione delle contromisure per la gestione dei rischi identificati, Definizione del Piano di Trattamento del Rischio.

**Cliente:** Acquirente Unico SpA - Roma

**Intervento:** Analisi dei Rischi IT e Piano di Trattamento dei Rischi nell'ambito del processo di implementazione di un SGSI ISO/IEC 27001 compliant.

**Attività svolte:** Censimento e classificazione degli Asset IT, Definizione dei livelli di impatto sul business, Identificazione delle minacce al patrimonio informativo e delle vulnerabilità degli Asset IT, Valutazione dei livelli di rischio, Identificazione delle contromisure per la gestione dei rischi identificati, Definizione del Piano di Trattamento del Rischio.

**Cliente:** Gruppo SOL - Monza

**Intervento:** Analisi dei Rischi IT e Piano di Trattamento dei Rischi nell'ambito del processo di implementazione di un SGSI ISO/IEC 27001 compliant.

**Attività svolte:** Censimento e classificazione degli Asset IT, Definizione dei livelli di impatto sul business, Identificazione delle minacce al patrimonio informativo e delle vulnerabilità degli Asset IT, Valutazione dei livelli di rischio, Identificazione delle contromisure per la gestione dei rischi identificati, Definizione del Piano di Trattamento del Rischio.

**Cliente:** ISED SpA - Roma

**Intervento:** Analisi dei Rischi IT e Piano di Trattamento dei Rischi nell'ambito del processo di implementazione di un SGSI ISO/IEC 27001 compliant.

**Attività svolte:** Censimento e classificazione degli Asset IT, Definizione dei livelli di impatto sul business, Identificazione delle minacce al patrimonio informativo e delle vulnerabilità degli Asset IT, Valutazione dei livelli di rischio, Identificazione delle contromisure per la gestione dei rischi identificati, Definizione del Piano di Trattamento del Rischio.

**Cliente:** Data Management SpA - Genova

**Intervento:** Analisi dei Rischi IT e Piano di Trattamento dei Rischi nell'ambito del processo di implementazione di un SGSI ISO/IEC 27001 compliant.

**Attività svolte:** Censimento e classificazione degli Asset IT, Definizione dei livelli di impatto sul business, Identificazione delle minacce al patrimonio informativo e delle vulnerabilità degli Asset IT, Valutazione dei livelli di rischio, Identificazione delle contromisure per la gestione dei rischi identificati, Definizione del Piano di Trattamento del Rischio.

**Cliente:** San Raffaele SpA - Roma

**Intervento:** Analisi dei Rischi IT e Piano di Trattamento dei Rischi nell'ambito del processo di implementazione di un SGSI ISO/IEC 27001 compliant.

**Attività svolte:** Censimento e classificazione degli Asset IT, Definizione dei livelli di impatto sul business, Identificazione delle minacce al patrimonio informativo e delle vulnerabilità degli Asset IT, Valutazione dei livelli di rischio, Identificazione delle contromisure per la gestione dei rischi identificati, Definizione del Piano di Trattamento del Rischio.

**Cliente:** ENAC - Roma

**Intervento:** Analisi dei Rischi IT secondo la metodologia CRAMM e supporto alla definizione di un Piano di Trattamento dei Rischi identificati.

**Attività svolte:** Censimento e classificazione degli Asset IT, Definizione dei livelli di impatto sul business, Identificazione delle minacce al patrimonio informativo e delle vulnerabilità degli Asset IT, Valutazione dei livelli di rischio mediante software tool (basato su metodologia CRAMM), Identificazione delle contromisure per la gestione dei rischi identificati, Definizione del Piano di Trattamento del Rischio.

---



## 7. Progettazione e supporto all'implementazione di SGSI ISO 27001 – 27017 – 27018

**Cliente:** BDO Italia Spa - Roma

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni in conformità alla normativa ISO 27001.

**Attività svolte:** Definizione della Politica per la sicurezza delle informazioni e del Campo di Applicazione, Analisi e Piano di Trattamento dei Rischi, Definizione della Dichiarazione di Applicabilità, Redazione delle procedure operative per la gestione delle informazioni, Definizione di report di Indicatori per SGSI, Redazione del Manuale del SGSI, Revisione del SGSI secondo il ciclo PDCA, Interfaccia con l'Ente di certificazione, Supporto all'adeguamento allo standard ISO/IEC 27001:2013.

**Cliente:** Gruppo Renco - Roma

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni in conformità alla normativa ISO 27001.

**Attività svolte:** Definizione della Politica per la sicurezza delle informazioni e del Campo di Applicazione, Analisi e Piano di Trattamento dei Rischi, Definizione della Dichiarazione di Applicabilità, Redazione delle procedure operative per la gestione delle informazioni, Definizione di report di Indicatori per SGSI, Redazione del Manuale del SGSI, Revisione del SGSI secondo il ciclo PDCA, Interfaccia con l'Ente di certificazione, Supporto all'adeguamento allo standard ISO/IEC 27001:2013.

**Cliente:** Capgemini Italia SpA - Roma

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni in conformità alla normativa ISO 27001 e alle linee guida ISO 27017 e ISO 27018 relative all'erogazione di servizi cloud.

**Attività svolte:** Definizione della Politica per la sicurezza delle informazioni e del Campo di Applicazione, Analisi e Piano di Trattamento dei Rischi, Definizione della Dichiarazione di Applicabilità, Redazione delle procedure operative per la gestione delle informazioni, Definizione di report di Indicatori per SGSI, Redazione del Manuale del SGSI, Revisione del SGSI secondo il ciclo PDCA, Supporto alla revisione dei contratti per l'erogazione di servizi cloud in conformità alle linee guida ISO 27017 e ISO 27018, Interfaccia con l'Ente di certificazione.

**Cliente:** Acquirente Unico - Roma

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni in conformità alla normativa ISO 27001.

**Attività svolte:** Definizione della Politica per la sicurezza delle informazioni e del Campo di Applicazione, Analisi e Piano di Trattamento dei Rischi, Definizione della Dichiarazione di Applicabilità, Redazione delle procedure operative per la gestione delle informazioni, Definizione di report di Indicatori per SGSI, Redazione del Manuale del SGSI, Revisione del SGSI secondo il ciclo PDCA, Interfaccia con l'Ente di certificazione, Supporto all'adeguamento allo standard ISO/IEC 27001:2013.

**Cliente: Gruppo SOL - Monza**

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni in conformità alla normativa ISO 27001 e alle linee guida ISO 27017 e ISO 27018 relative all'erogazione di servizi cloud.

**Attività svolte:** Definizione della Politica per la sicurezza delle informazioni e del Campo di Applicazione, Analisi e Piano di Trattamento dei Rischi, Definizione della Dichiarazione di Applicabilità, Redazione delle procedure operative per la gestione delle informazioni, Definizione di report di Indicatori per SGSI, Redazione del Manuale del SGSI, Revisione del SGSI secondo il ciclo PDCA, Supporto alla revisione dei contratti per l'erogazione di servizi cloud in conformità alle linee guida ISO 27017 e ISO 27018, Interfaccia con l'Ente di certificazione.

**Cliente: Sermetra Net Service S.r.l. - Roma**

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni in conformità alla normativa ISO 27001.

**Attività svolte:** Definizione della Politica per la sicurezza delle informazioni e del Campo di Applicazione, Analisi e Piano di Trattamento dei Rischi, Definizione della Dichiarazione di Applicabilità, Redazione delle procedure operative per la gestione delle informazioni, Definizione di report di Indicatori per SGSI, Redazione del Manuale del SGSI, Revisione del SGSI secondo il ciclo PDCA, Interfaccia con l'Ente di certificazione.

**Cliente: Wichee Srl – Cinisello Balsamo**

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni in conformità alla normativa ISO 27001.

**Attività svolte:** Definizione della Politica per la sicurezza delle informazioni e del Campo di Applicazione, Analisi e Piano di Trattamento dei Rischi, Definizione della Dichiarazione di Applicabilità, Redazione delle procedure operative per la gestione delle informazioni, Definizione di report di Indicatori per SGSI, Redazione del Manuale del SGSI, Revisione del SGSI secondo il ciclo PDCA, Interfaccia con l'Ente di certificazione.

**Cliente: ISED SpA - Roma**

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni in conformità alla normativa ISO 27001. e alle linee guida ISO 27017 e ISO 27018 relative all'erogazione di servizi cloud.

**Attività svolte:** Definizione della Politica per la sicurezza delle informazioni e del Campo di Applicazione, Analisi e Piano di Trattamento dei Rischi, Definizione della Dichiarazione di Applicabilità, Redazione delle procedure operative per la gestione delle informazioni, Definizione di report di Indicatori per SGSI, Redazione del Manuale del SGSI, Revisione del SGSI secondo il ciclo PDCA, Supporto alla revisione dei contratti per l'erogazione di servizi cloud in conformità alle linee guida ISO 27017 e ISO 27018, Interfaccia con l'Ente di certificazione.

**Cliente: Data Management SpA - Genova/Brindisi/Imola**

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni in conformità alla normativa ISO 27001.

**Attività svolte:** Definizione della Politica per la sicurezza delle informazioni e del Campo di Applicazione, Analisi e Piano di Trattamento dei Rischi, Definizione della Dichiarazione di Applicabilità, Redazione delle procedure operative per la gestione delle informazioni, Definizione di report di Indicatori per SGSI, Redazione del Manuale del SGSI, Revisione del SGSI secondo il ciclo PDCA, Interfaccia con l'Ente di certificazione.

**Cliente: San Raffaele SpA - Roma**

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni in conformità alla normativa ISO 27001.

**Attività svolte:** Definizione della Politica per la sicurezza delle informazioni e del Campo di Applicazione, Analisi e Piano di Trattamento dei Rischi, Definizione della Dichiarazione di Applicabilità, Redazione delle procedure operative per la gestione delle informazioni, Definizione di report di Indicatori per SGSI, Redazione del Manuale del SGSI, Revisione del SGSI secondo il ciclo PDCA, Interfaccia con l'Ente di certificazione.

**Cliente: YoctoIT Srl - Monza**

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione integrato Qualità ISO 9001:2015 – Sicurezza delle Informazioni ISO/IEC 27001:2013.

**Attività svolte:** Definizione della Politica per la sicurezza delle informazioni e del Campo di Applicazione, Analisi e Piano di Trattamento dei Rischi, Definizione della Dichiarazione di Applicabilità, Redazione delle procedure operative per la gestione delle informazioni, Definizione di report di Indicatori per SGSI, Redazione del Manuale del SGSI, Revisione del SGSI secondo il ciclo PDCA,. Definizione della Politica per la qualità, Redazione delle procedure operative per la gestione della qualità, Definizione di report di Indicatori per SGQ, Redazione del Manuale del SGQ, Redazione della modulistica per la qualità, Revisione del SGQ secondo il ciclo PDCA. Interfaccia con l'Ente di certificazione.

**Cliente: BinHexS Srl - Milano**

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione integrato Qualità ISO 9001:2015 – Sicurezza delle Informazioni ISO/IEC 27001:2013.

**Attività svolte:** Definizione della Politica per la sicurezza delle informazioni e del Campo di Applicazione, Analisi e Piano di Trattamento dei Rischi, Definizione della Dichiarazione di Applicabilità, Redazione delle procedure operative per la gestione delle informazioni, Definizione di report di Indicatori per SGSI, Redazione del Manuale del SGSI, Revisione del SGSI secondo il ciclo PDCA,. Definizione della Politica per la qualità, Redazione delle procedure operative per la gestione della qualità, Definizione di report di Indicatori per SGQ, Redazione del Manuale del SGQ, Redazione della modulistica per la qualità, Revisione del SGQ secondo il ciclo PDCA. Interfaccia con l'Ente di certificazione.

## 8. Progettazione e supporto all'implementazione di SGQ ISO 9001

**Cliente:** BSD Srl - Roma

**Intervento:** Implementazione di un Sistema di Gestione della Qualità in conformità alla normativa ISO 9001.

**Attività svolte:** Definizione della Politica per la qualità, Redazione delle procedure operative per la gestione della qualità, Definizione di report di Indicatori per SGQ, Redazione del Manuale del SGQ, Redazione della modulistica per la qualità, Revisione del SGQ secondo il ciclo PDCA, Interfaccia con l'Ente di certificazione.

**Cliente:** Welikecrm Srl - Roma

**Intervento:** Implementazione di un Sistema di Gestione della Qualità in conformità alla normativa ISO 9001.

**Attività svolte:** Definizione della Politica per la qualità, Redazione delle procedure operative per la gestione della qualità, Definizione di report di Indicatori per SGQ, Redazione del Manuale del SGQ, Redazione della modulistica per la qualità, Revisione del SGQ secondo il ciclo PDCA, Interfaccia con l'Ente di certificazione.

**Cliente:** AMC Services Srl - Roma

**Intervento:** Implementazione di un Sistema di Gestione della Qualità in conformità alla normativa ISO 9001.

**Attività svolte:** Definizione della Politica per la qualità, Redazione delle procedure operative per la gestione della qualità, Definizione di report di Indicatori per SGQ, Redazione del Manuale del SGQ, Redazione della modulistica per la qualità, Revisione del SGQ secondo il ciclo PDCA, Interfaccia con l'Ente di certificazione.

**Cliente:** Atleticom Srl - Roma

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione della Qualità in conformità alla normativa ISO 9001.

**Attività svolte:** Definizione della Politica per la qualità, Redazione delle procedure operative per la gestione della qualità, Definizione di report di Indicatori per SGQ, Redazione del Manuale del SGQ, Redazione della modulistica per la qualità, Revisione del SGQ secondo il ciclo PDCA, Interfaccia con l'Ente di certificazione.

**Cliente:** Balance Srl - Milano

**Intervento:** Implementazione di un Sistema di Gestione della Qualità in conformità alla normativa ISO 9001.

**Attività svolte:** Definizione della Politica per la qualità, Redazione delle procedure operative per la gestione della qualità, Definizione di report di Indicatori per SGQ, Redazione del Manuale del SGQ, Redazione della modulistica per la qualità, Revisione del SGQ secondo il ciclo PDCA, Interfaccia con l'Ente di certificazione.

**Cliente: Gruppo SOL – Monza**

**Intervento:** Definizione del Modello di Risk Management in ambito qualità conforme allo standard EN ISO 9001:2015

**Attività svolte:** Definizione della metodologia e del processo di Risk Assessment per processi e progetti, Definizione della procedura di governo, Supporto al mapping dei processi aziendali, Identificazione dei principali eventi di rischi.

**Cliente: YoctoIT Srl - Milano**

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione integrato Qualità ISO 9001:2015 – Sicurezza delle Informazioni ISO/IEC 27001:2013.

**Attività svolte:** Definizione della Politica per la sicurezza delle informazioni e del Campo di Applicazione, Analisi e Piano di Trattamento dei Rischi, Definizione della Dichiarazione di Applicabilità, Redazione delle procedure operative per la gestione delle informazioni, Definizione di report di Indicatori per SGSI, Redazione del Manuale del SGSI, Revisione del SGSI secondo il ciclo PDCA,. Definizione della Politica per la qualità, Redazione delle procedure operative per la gestione della qualità, Definizione di report di Indicatori per SGQ, Redazione del Manuale del SGQ, Redazione della modulistica per la qualità, Revisione del SGQ secondo il ciclo PDCA. Interfaccia con l'Ente di certificazione.

**Cliente: BinHexS Srl - Milano**

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione integrato Qualità ISO 9001:2015 – Sicurezza delle Informazioni ISO/IEC 27001:2013.

**Attività svolte:** Definizione della Politica per la sicurezza delle informazioni e del Campo di Applicazione, Analisi e Piano di Trattamento dei Rischi, Definizione della Dichiarazione di Applicabilità, Redazione delle procedure operative per la gestione delle informazioni, Definizione di report di Indicatori per SGSI, Redazione del Manuale del SGSI, Revisione del SGSI secondo il ciclo PDCA,. Definizione della Politica per la qualità, Redazione delle procedure operative per la gestione della qualità, Definizione di report di Indicatori per SGQ, Redazione del Manuale del SGQ, Redazione della modulistica per la qualità, Revisione del SGQ secondo il ciclo PDCA. Interfaccia con l'Ente di certificazione.

**Cliente: Capgemini Italia SpA - Roma**

**Intervento:** Progettazione e supporto all'implementazione di un Sistema di Gestione integrato Qualità ISO 9001:2015 – Sicurezza delle Informazioni ISO/IEC 27001:2013.

**Attività svolte:** Definizione della Politica per la sicurezza delle informazioni e del Campo di Applicazione, Analisi e Piano di Trattamento dei Rischi, Definizione della Dichiarazione di Applicabilità, Redazione delle procedure operative per la gestione delle informazioni, Definizione di report di Indicatori per SGSI, Redazione del Manuale del SGSI, Revisione del SGSI secondo il ciclo PDCA,. Definizione della Politica per la qualità, Redazione delle procedure operative per la gestione della qualità, Definizione di report di Indicatori per SGQ, Redazione del Manuale del SGQ, Redazione della modulistica per la qualità, Revisione del SGQ secondo il ciclo PDCA. Interfaccia con l'Ente di certificazione.

---

**Cliente:** Acquedotto Lucano SpA - Potenza

**Intervento:** Implementazione di un Sistema di Gestione della Qualità in conformità alla normativa ISO 9001.

**Attività svolte:** Definizione della Politica per la qualità, Redazione delle procedure operative per la gestione della qualità, Definizione di report di Indicatori per SGQ, Redazione del Manuale del SGQ, Redazione della modulistica per la qualità, Revisione del SGQ secondo il ciclo PDCA, Interfaccia con l'Ente di certificazione

---

---

## 9. Progettazione e supporto all'implementazione di SGS ISO 20000

### Cliente: Trenitalia SpA

**Intervento:** Supporto all'implementazione del Sistema di Gestione dei Servizi (SGS) aziendale ed esecuzione di Audit di Prima Parte finalizzati alla verifica della conformità del Sistema SGS ai requisiti dello standard internazionale ISO 20000 relativo alla gestione dei servizi IT.

**Attività svolte:** Analisi dell'impianto di Policy e Procedure, dei processi di gestione dei servizi IT, Interviste a risorse coinvolte nei processi di gestione dei servizi IT, Gap Analysis rispetto ai requisiti ISO 20000, Definizione delle Azioni di Adeguamento del SGS, Raccolta delle evidenze sul campo, Redazione del Report di Audit, Formalizzazione delle Non Conformità, delle Raccomandazioni e delle Osservazioni, Monitoraggio dell'attuazione delle Azioni Correttive e Preventive stabilite.

### Cliente: Gruppo Intersistemi

**Intervento:** Supporto all'implementazione del Sistema di Gestione dei Servizi (SGS) aziendale ed esecuzione di Audit di Prima Parte finalizzati alla verifica della conformità del Sistema SGS ai requisiti dello standard internazionale ISO 20000 relativo alla gestione dei servizi IT.

**Attività svolte:** Analisi dell'impianto di Policy e Procedure, dei processi di gestione dei servizi IT, Interviste a risorse coinvolte nei processi di gestione dei servizi IT, Gap Analysis rispetto ai requisiti ISO 20000, Definizione delle Azioni di Adeguamento del SGS, Raccolta delle evidenze sul campo, Redazione del Report di Audit, Formalizzazione delle Non Conformità, delle Raccomandazioni e delle Osservazioni, Monitoraggio dell'attuazione delle Azioni Correttive e Preventive stabilite

### Cliente: Capgemini Italia Spa - Roma

**Intervento:** Supporto all'implementazione del Sistema di Gestione dei Servizi (SGS) aziendale in conformità ai requisiti dello standard internazionale ISO 20000 relativo alla gestione dei servizi IT.

**Attività svolte:** Analisi dell'impianto di Policy e Procedure, dei processi di gestione dei servizi IT, Interviste a risorse coinvolte nei processi di gestione dei servizi IT, Gap Analysis rispetto ai requisiti ISO 20000, Definizione delle Azioni di Adeguamento del SGS, Redazione delle politiche richieste dallo standard ISO/IEC 20000, Redazione del piano di gestione del servizio, Redazione dei piani di capacità, disponibilità, continuità, Supporto alla definizione del catalogo dei servizi, degli SLA e degli OLA, Raccolta delle evidenze sul campo, Redazione del Report di Audit, Formalizzazione delle Non Conformità, delle Raccomandazioni e delle Osservazioni, Monitoraggio dell'attuazione delle Azioni Correttive e Preventive stabilite



---

## 10. Security Assessment & Monitoring: Penetration test & Vulnerability Assessment

### Vari Clienti

**Intervento:** Analisi, valutazione e presentazione dei rischi derivanti dallo sfruttamento delle vulnerabilità tecnologiche nell'ambito di un ambiente applicativo Web utilizzato da un provider di servizi internazionale per i clienti (Assist Spa, Gruppo SOL, RCS Media Group Spa, Guess Service Srl, San Raffale Spa, Fendi Spa, Acquirente Unico)

**Attività svolte:** Conduzione di Web Application Penetration Test, Presentazione del rapporto di audit con remediation plan, Attività di social engineering.

---

## 11. Logical Security Controls System Configuration

### Cliente: Guess Service Srl – Firenze - Lugano

**Intervento:** Definizione e stesura di linee guida e procedure per analizzare, identificare e proteggere i Configuration Item (CI) che compongono i servizi applicativi ed infrastrutturali aziendali.

**Attività svolte:** Analisi della configurazione dei principali Configuration Item (CI) aziendali (apparati di networking, Sistemi Operativi, RDBMS, Application Server, Servizi Middleware, Servizi di Frontend), Documentazione dei Configuration Item e delle interrelazioni, Individuazione delle principali aree di rischio, Definizione di linee guida e procedure di configurazione dei CI ai fini di un corretto hardening.

### Cliente: Enel SpA - Roma

**Intervento:** Definizione e stesura di linee guida e procedure per analizzare, identificare e proteggere i Configuration Item (CI) che compongono i servizi applicativi ed infrastrutturali aziendali.

**Attività svolte:** Analisi della configurazione dei principali Configuration Item (CI) aziendali (apparati di networking, Sistemi Operativi, RDBMS, Application Server, Servizi Middleware, Servizi di Frontend), Documentazione dei Configuration Item e delle interrelazioni, Individuazione delle principali aree di rischio, Definizione di linee guida e procedure di configurazione dei CI ai fini di un corretto hardening.

### Cliente: Birra Peroni SpA - Roma

**Intervento:** Definizione e stesura di linee guida e procedure per analizzare, identificare e proteggere i Configuration Item (CI) che compongono i servizi applicativi ed infrastrutturali aziendali.

**Attività svolte:** Analisi della configurazione dei principali Configuration Item (CI) aziendali (apparati di networking, Sistemi Operativi, RDBMS, Application Server, Servizi Middleware, Servizi di Frontend), Documentazione dei Configuration Item e delle interrelazioni, Individuazione delle principali aree di rischio, Definizione di linee guida e procedure di configurazione dei CI ai fini di un corretto hardening.

---

## 12. Logical Security Controls Account & User Management

**Cliente:** ATAC SpA - Roma

**Intervento:** IT Assessment sul sistema di controllo degli accessi e sul sistema di autorizzazione relativamente agli applicativi ed ai sistemi aziendali (Segregation of Duties).

**Attività svolte:** Verifica dei processi di gestione degli user profile, delle matrici profili/funzionalità, del processo di controllo degli accessi ai sistemi informativi ai fini di una corretta Segregation of Duties, Individuazione delle principali aree di rischio e delle Azioni Correttive per la loro mitigazione.

**Cliente:** Enel SpA - Roma

**Intervento:** IT Assessment sul sistema di controllo degli accessi e sul sistema di autorizzazione relativamente agli applicativi ed ai sistemi aziendali (Segregation of Duties).

**Attività svolte:** Verifica dei processi di gestione degli user profile, delle matrici profili/funzionalità, del processo di controllo degli accessi ai sistemi informativi ai fini di una corretta Segregation of Duties, Individuazione delle principali aree di rischio e delle Azioni Correttive per la loro mitigazione.

**Cliente:** Poste Italiane SpA - Roma

**Intervento:** IT Assessment sul sistema di controllo degli accessi e sul sistema di autorizzazione relativamente agli applicativi ed ai sistemi aziendali (Segregation of Duties).

**Attività svolte:** Verifica dei processi di gestione degli user profile, delle matrici profili/funzionalità, del processo di controllo degli accessi ai sistemi informativi ai fini di una corretta Segregation of Duties, Individuazione delle principali aree di rischio e delle Azioni Correttive per la loro mitigazione.

---

### 13. Incident Management

**Cliente:** Guess Service Srl - Firenze

**Intervento:** Supporto alla progettazione del Service Desk della Divisione IT secondo le “good practice” ITIL v3.

**Attività svolte:** Analisi AS IS del modello aziendale di gestione di IT Incident e IT Service Request, Progettazione di un modello basato su ITIL v3, Disegno dei flussi operativi, Supporto alla customization e test dell’applicativo a supporto dei processi

**Cliente:** San Raffaele SpA– Roma

**Intervento:** Supporto alla progettazione del Service Desk della Divisione IT secondo le “good practice” ITIL v3.

**Attività svolte:** Analisi AS IS del modello aziendale di gestione di IT Incident e IT Service Request, Progettazione di un modello basato su ITIL v3, Disegno dei flussi operativi, Supporto alla customization e test dell’applicativo a supporto dei processi.

---

## 14. Business Continuity Plan

**Cliente:** Gruppo SOL - Monza

**Intervento:** Analisi strategiche per la pianificazione della continuità operativa e di servizio.

**Attività svolte:** Censimento dei processi critici per la continuità del business aziendale, Conduzione della Business Impact Analysis.

**Cliente:** Acquirente Unico - Roma

**Intervento:** Analisi strategiche per la pianificazione della continuità operativa e di servizio.

**Attività svolte:** Censimento dei processi critici per la continuità del business aziendale, Conduzione della Business Impact Analysis.

**Cliente:** Capgemini Italia SpA - Roma

**Intervento:** Analisi strategiche per la pianificazione della continuità operativa e di servizio.

**Attività svolte:** Censimento dei processi critici per la continuità del business aziendale, Conduzione della Business Impact Analysis.

**Cliente:** Kuwait Petroleum Italia S.p.A. - Roma

**Intervento:** Analisi strategiche per la pianificazione della continuità operativa e di servizio.

**Attività svolte:** Censimento dei processi critici per la continuità del business aziendale, Conduzione della Business Impact Analysis, Redazione del Disaster Recovery Plan, Supporto per il Test dei Piani di Business Continuity e Disaster Recovery.

**Cliente:** San Raffaele SpA - Roma

**Intervento:** Analisi strategiche per la pianificazione della continuità operativa e di servizio.

**Attività svolte:** Censimento dei processi critici per la continuità del business aziendale, Conduzione della Business Impact Analysis.

**Cliente:** Enel SpA - Roma

**Intervento:** Analisi strategiche per la pianificazione della continuità operativa e di servizio.

**Attività svolte:** Censimento dei processi critici per la continuità del business aziendale, Conduzione della Business Impact Analysis, Redazione del Disaster Recovery Plan, Supporto per il Test dei Piani di Business Continuity e Disaster Recovery.

---

**Cliente: Capgemini Italia - Roma**

**Intervento:** Analisi strategiche per la pianificazione della continuità operativa e di servizio.

**Attività svolte:** Censimento dei processi critici per la continuità del business aziendale, Conduzione della Business Impact Analysis, Redazione del Disaster Recovery Plan, Supporto per il Test dei Piani di Business Continuity e Disaster Recovery.

---

**Cliente: Guess Service Srl - Firenze**

**Intervento:** Analisi strategiche per la pianificazione della continuità operativa e di servizio.

**Attività svolte:** Censimento dei processi critici per la continuità del business aziendale, Conduzione della Business Impact Analysis.

---

**Cliente: Birra Peroni SpA - Roma**

**Intervento:** Analisi strategiche per la pianificazione della continuità operativa e di servizio.

**Attività svolte:** Censimento dei processi critici per la continuità del business aziendale, Conduzione della Business Impact Analysis, Redazione del Disaster Recovery Plan, Supporto per il Test dei Piani di Business Continuity e Disaster Recovery.

---

**Cliente: Gruppo SOL - Monza**

**Intervento:** Progettazione e supporto all'implementazione di un Business Continuity Management System in conformità alla normativa ISO 22301.

**Attività svolte:** Definizione della Politica per la continuità operativa e del Campo di Applicazione, Business Impact Analysis, Analisi e Piano di Trattamento dei Rischi, Definizione delle strategie di continuità, Redazione dei piani di Business Continuity / Disaster Recovery, Definizione di report di Indicatori per il BCMS, Supporto nelle attività di test del Business Continuity Plan, Revisione del BCMS secondo il ciclo PDCA, Interfaccia con l'Ente di certificazione.

---

## 15.Security Awareness

**Cliente:** Capgemini Italia SpA - Roma

**Intervento:** Corsi di sensibilizzazione e formazione sulla Sicurezza delle Informazioni secondo la norma ISO/IEC 27001:2013.

**Attività svolte:** Excursus sui principali rischi IT presenti nei contesti aziendali, Descrizione delle procedure operative del SGSI, Illustrazione dei principali aspetti della norma ISO/IEC 27001:2013, Illustrazione delle principali implicazioni organizzative dell'implementazione di un SGSI.

**Cliente:** Acquirente Unico - Roma

**Intervento:** Corsi di formazione sulla Sicurezza delle Informazioni secondo la norma ISO/IEC 27001:2013.

**Attività svolte:** Illustrazione dei principali aspetti della norma ISO/IEC 27001:2013 (High Level Structure, Annex A), Illustrazione delle principali implicazioni organizzative dell'implementazione di un SGSI

**Cliente:** Gruppo SOL- Monza

**Intervento:** Corso di certificazione ITIL V3.

**Attività svolte:** Descrizione dei contenuti del frame work ITIL - Information Technology Infrastructure Library (Service Strategy, Service Design, Service Transition, Service Operation, Continual Improvement), Esercitazioni e Casi Pratici, Esame Finale.

**Cliente:** Gruppo SOL - Monza

**Intervento:** Corsi di certificazione Lead Auditor ISO/IEC 27001:2005.

**Attività svolte:** Descrizione dei contenuti della Norma ISO/IEC 27001 (Impianto Documentale, Punti della Norma, Controlli), Introduzione allo standard di Audit ISO 19011, Esercitazioni e Casi Pratici, Esame Finale.

**Cliente:** Data Management – Genova

**Intervento:** Corso di certificazione ITIL V3.

**Attività svolte:** Descrizione dei contenuti del frame work ITIL - Information Technology Infrastructure Library (Service Strategy, Service Design, Service Transition, Service Operation, Continual Improvement), Esercitazioni e Casi Pratici, Esame Finale.

**Cliente:** Data Management – Genova**Intervento:** Corsi di certificazione Lead Auditor ISO/IEC 27001:2005.**Attività svolte:** Descrizione dei contenuti della Norma ISO/IEC 27001 (Impianto Documentale, Punti della Norma, Controlli), Introduzione allo standard di Audit ISO 19011, Esercitazioni e Casi Pratici, Esame Finale.**Cliente:** San Raffaele SpA - Roma**Intervento:** Corsi di certificazione Lead Auditor ISO/IEC 27001:2005.**Attività svolte:** Descrizione dei contenuti della Norma ISO/IEC 27001 (Impianto Documentale, Punti della Norma, Controlli), Introduzione allo standard di Audit ISO 19011, Esercitazioni e Casi Pratici, Esame Finale.**Cliente:** San Raffaele SpA - Roma**Intervento:** Corso di certificazione ITIL V3.**Attività svolte:** Descrizione dei contenuti del framework ITIL - Information Technology Infrastructure Library (Service Strategy, Service Design, Service Transition, Service Operation, Continual Improvement), Esercitazioni e Casi Pratici, Esame Finale.**Cliente:** Guess Service - Firenze**Intervento:** Corso di certificazione ITIL V3.**Attività svolte:** Descrizione dei contenuti del framework ITIL - Information Technology Infrastructure Library (Service Strategy, Service Design, Service Transition, Service Operation, Continual Improvement), Esercitazioni e Casi Pratici, Esame Finale.**Cliente:** San Raffaele SpA - Roma**Intervento:** Corsi di sensibilizzazione e formazione sulla Sicurezza delle Informazioni secondo la norma ISO/IEC 27001:2005.**Attività svolte:** Excursus sui principali rischi IT presenti nei contesti aziendali, Descrizione delle procedure operative del SGSI, Illustrazione dei principali aspetti della norma ISO/IEC 27001, Illustrazione delle principali implicazioni organizzative dell'implementazione di un SGSI.**Cliente:** Birra Peroni SpA - Roma**Intervento:** Corsi di certificazione Lead Auditor ISO/IEC 27001:2005.**Attività svolte:** Descrizione dei contenuti della Norma ISO/IEC 27001 (Impianto Documentale, Punti della Norma, Controlli), Introduzione allo standard di Audit ISO 19011, Esercitazioni e Casi Pratici, Esame Finale.



---

## 16. Modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001

**Cliente:** ISED SpA - Roma

**Intervento:** Revisione del Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001.

**Attività svolte:** Analisi del Modello di organizzazione e controllo esistente, revisione della mappatura rischi/reato ex D.Lgs. 231/2001, Revisione Analisi dei Rischi, Valutazione del disegno del sistema a presidio dei rischi/reati, Revisione del Disegno del Modello di Organizzazione e Controllo e dei Protocolli etico-organizzativi, Monitoraggio del Modello.

**Cliente:** Leitwind Service Srl - Avellino

**Intervento:** Revisione del Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001.

**Attività svolte:** Analisi del Modello di organizzazione e controllo esistente, revisione della mappatura rischi/reato ex D.Lgs. 231/2001, Revisione Analisi dei Rischi, Valutazione del disegno del sistema a presidio dei rischi/reati, Revisione del Disegno del Modello di Organizzazione e Controllo e dei Protocolli etico-organizzativi, Monitoraggio del Modello.

**Cliente:** Varie Aziende Pubbliche e Private di diversi settori

**Intervento:** Progettazione ed Implementazione di un Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs 231/2001.

**Attività svolte:** Analisi del Modello di organizzazione e controllo esistente, Realizzazione della mappatura rischi/reato ex D.Lgs. 231/2001, Valutazione del disegno del sistema a presidio dei rischi/reati, Disegno del Modello di Organizzazione e Controllo, Redazione del Codice Etico e dei Protocolli etico-organizzativi, Monitoraggio del Modello.

**Cliente:** Varie Aziende Pubbliche e Private di diversi settori

**Intervento:** Revisione del Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001.

**Attività svolte:** Analisi del Modello di organizzazione e controllo esistente, revisione della mappatura rischi/reato ex D.Lgs. 231/2001, Revisione Analisi dei Rischi, Valutazione del disegno del sistema a presidio dei rischi/reati, Revisione del Disegno del Modello di Organizzazione e Controllo e dei Protocolli etico-organizzativi, Monitoraggio del Modello.

---

## 17.IT Governance

**Cliente:** Kering Group - Firenze

**Intervento:** Progettazione del processo di comunicazione per la gestione dei Critical Incident e delle finestre di Maintenance.

**Attività svolte:** Analisi dei requisiti, Rappresentazione del processo, Identificazione Issue, Open Point e Opportunità di Miglioramento, Redazione delle procedure, Condivisione con i referenti aziendali.

**Cliente:** Kering Group - Firenze

**Intervento:** Progettazione di una Dashboard di indicatori di efficacia ed efficienza dei Servizi IT.

**Attività svolte:** Definizione del perimetro di analisi, Analisi dei servizi oggetto delle misurazioni, Identificazione dei CSF (Critical Success Factor), Identificazione dei KPI (Key Performance Indicator), Progettazione di una Dashboard di indicatori di servizio secondo le good practice di ITIL v3.

**Cliente:** Banca Mediolanum - Milano

**Intervento:** Revisione Contratto di Full Outsourcing Banca Mediolanum – Cedacri

**Attività svolte:** Analisi critica della componente tecnica contenuta nel contratto di outsourcing dei servizi applicativi di Banca Mediolanum gestiti da Cedacri (aspetti tecnici contrattuali di natura IT, costi, livelli di servizio, analisi rischi, ecc...)

**Cliente:** Acquedotto Pugliese - Bari

**Intervento:** Reengineering della Funzione Sistemi Informativi aziendali.

**Attività svolte:** Analisi AS IS della struttura organizzativa della Funzione Sistemi Informativi aziendali e dei relativi processi a supporto della gestione dell'infrastruttura tecnologica aziendale e dei servizi IT, Individuazione delle criticità e delle opportunità di miglioramento, Definizione del Modello TO BE dei processi secondo il framework ITIL v.3, Supporto alla pianificazione ed implementazione delle Azioni di Miglioramento.

**Cliente:** AMA SPA - Roma

**Intervento:** Quality Assurance implementazione soluzione SAP ECC.

**Attività svolte:** Verifica Qualità della realizzazione SAP – in termini di allineamento dei documenti di design applicativo prodotti dal system integrator (Application Blueprint, Configurazione, Analisi Funzionali, etc..) rispetto a quanto riportato nei requisiti di business formalizzati da AMA. Controllo della esaustività / efficacia degli scenari di Demo SAP proposti dal system integrator e supporto attivo ai Key User nella validazione delle relative sessioni.

**Cliente:** Gruppo SOL - Monza

**Intervento:** Progettazione di una Dashboard di indicatori di efficacia ed efficienza dei Servizi IT.

**Attività svolte:** Definizione del perimetro di analisi, Analisi dei servizi oggetto delle misurazioni, Identificazione dei CSF (Critical Success Factor), Identificazione dei KPI (Key Performance Indicator), Progettazione di una Dashboard di indicatori di servizio secondo le good practice esistenti.

## 18.Data Integrity – Data Governance – Data Quality

**Cliente:** Gruppo SOL - Monza

**Intervento:** Implementazione di un Sistema di Gestione di Data Integrity.

**Attività svolte:** Attività di pianificazione mediante chiarificazione degli obiettivi del progetto, definizione dei tempi, delle responsabilità e delle risorse necessarie, Elaborazione di un documento che definisca la politica aziendale in tema di integrità dei dati (data governance) e, conseguentemente, nell'ambito del Sistema di Gestione Integrato, la relativa Direttiva, Identificazione dei sistemi GMP, Mappatura dei processi in ambito applicativi software GMP presenti presso la Sede di Monza del Gruppo SOL, processi primari sul campo presso una sede campione ASU n, processi secondari, Identificazione dei record a rilevanza GMP, Metodiche di Quality Risk Management applicate ai record GMP, Verifica Conformità MHRA (ALCOA+CCEA) e Audit di I° Parte con rilevazione eventuali Non Conformità, Elaborazione di un Piano di Remediation, Adeguamento Modello Organizzativo e Adeguamento Procedurale, Formazione generale e/o specifica, Adeguamento/Miglioramento Workflow esistenti, Adeguamento/Miglioramento Tecnologie esistenti, Definizione metriche per il monitoraggio ed il controllo dell'integrità dei dati (Quality Metrics).

**Cliente:** Credito Fondiario - Roma

**Intervento:** Progetto in ambito Data Governance / Data Quality.

**Attività svolte:** Redazione delle Procedure e delle Policy di Data Governance, Definizione processo di dettaglio e presidi organizzativi per la gestione del dato, definizione di regole che consentano la validazione dei dati all'interno DWH aziendale ai fini di analisi e reporting allineati con le regole di data quality definite, Analisi del dominio dati e identificazione degli owner e delle modalità di gestione.