

La gestione del rischio e l'approccio della soluzione RiS nell'ambito del nuovo Regolamento Europeo

Ing. Alessandro Cerasoli

IT Governance Practice Manager NIS - Network Integration and Solutions S.r.l.

DATA PROTECTION & GDPR

Misure di sicurezza informatiche ed assicurative nel trattamento dei dati personali

25 OTTOBRE 2016

Data breach



- **Notifica al Garante Privacy - Articolo 33**

In caso di violazione dei dati personali, notifica della violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore

- **Comunicazione agli Interessati - Articolo 34**

In caso di **rischi** elevati per i diritti e le libertà fondamentali degli individui, senza ingiustificato ritardo



Impegni, responsabilità, oneri

- **Sanzioni amministrative elevate – Articolo 83**

Sanzioni amministrative pecuniarie fino a 20M EUR o, per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente



- **Sanzioni penali**

Le sanzioni penali rimangono di competenza di ogni singolo Stato



Aumento degli obblighi

- **Ruolo del Data Protection Officer (DPO)** — Articolo 39
 - Sensibilizzare
 - Controllare e vigilare
 - Fornire supporto strategico
 - Essere punto di contatto con il Garante
 - Considerare i **rischi** associati a tutte le fasi di trattamento
- **Protection by Design** — Articolo 25
 - Principi e politiche
- **Data Protection Impact Assessment** — Articolo 35
 - Valutazione dell’impatto dei trattamenti nelle situazioni in cui si possa presentare un **rischio** elevato per i diritti e le libertà delle persone fisiche

La novità... O forse solo una conferma...

- ...aver valutato la *probabilità* che la violazione dei dati personali presenti un *rischio* elevato
- ...ridurre al *minimo* il trattamento dei dati personali conformemente ai principi di proporzionalità e di necessità
- Quando un tipo di trattamento, [...] può presentare un *rischio* elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, [...] una *valutazione dell'impatto* dei trattamenti previsti sulla protezione dei dati personali
- ... la valutazione d'impatto sulla protezione dei dati [...] indichi che il trattamento presenterebbe un *rischio* elevato in assenza di *misure* adottate dal titolare del trattamento per *attenuare il rischio*



Necessità di definire un approccio sistematico (metodologico) orientato alla identificazione e valutazione dei rischi per poter consapevolmente adottare le contromisure sufficienti ai fini della garanzia della protezione e tutela dei dati personali comprensivi della libera circolazione di tali dati



Approccio metodologico

GOVERNANCE

- Definire una **Policy di Personal Data Protection** – Protection by design
- Identificare un **Inventario dei Dati Personali** e dei flussi che li interessano (relazioni)
- Includere la **Data Protection** nei trattamenti

GESTIONE

- Gestire i Rischi (DPIA e analisi dei rischi)
- Definire programmi di formazione e sensibilizzazione
- Impostare le attività per ottemperare agli obiettivi ed alle iniziative di Data Protection (rispondere alla policy)
- Attivare procedure per supportare le parti interessate (protezione, gestione comunicazione)
- Monitorare novità o modifiche nei Processi e nelle Procedure
- Gestire le eccezioni/incident (Personal Data Breach)
- Monitorare le modalità di trattamento dei Dati Personali



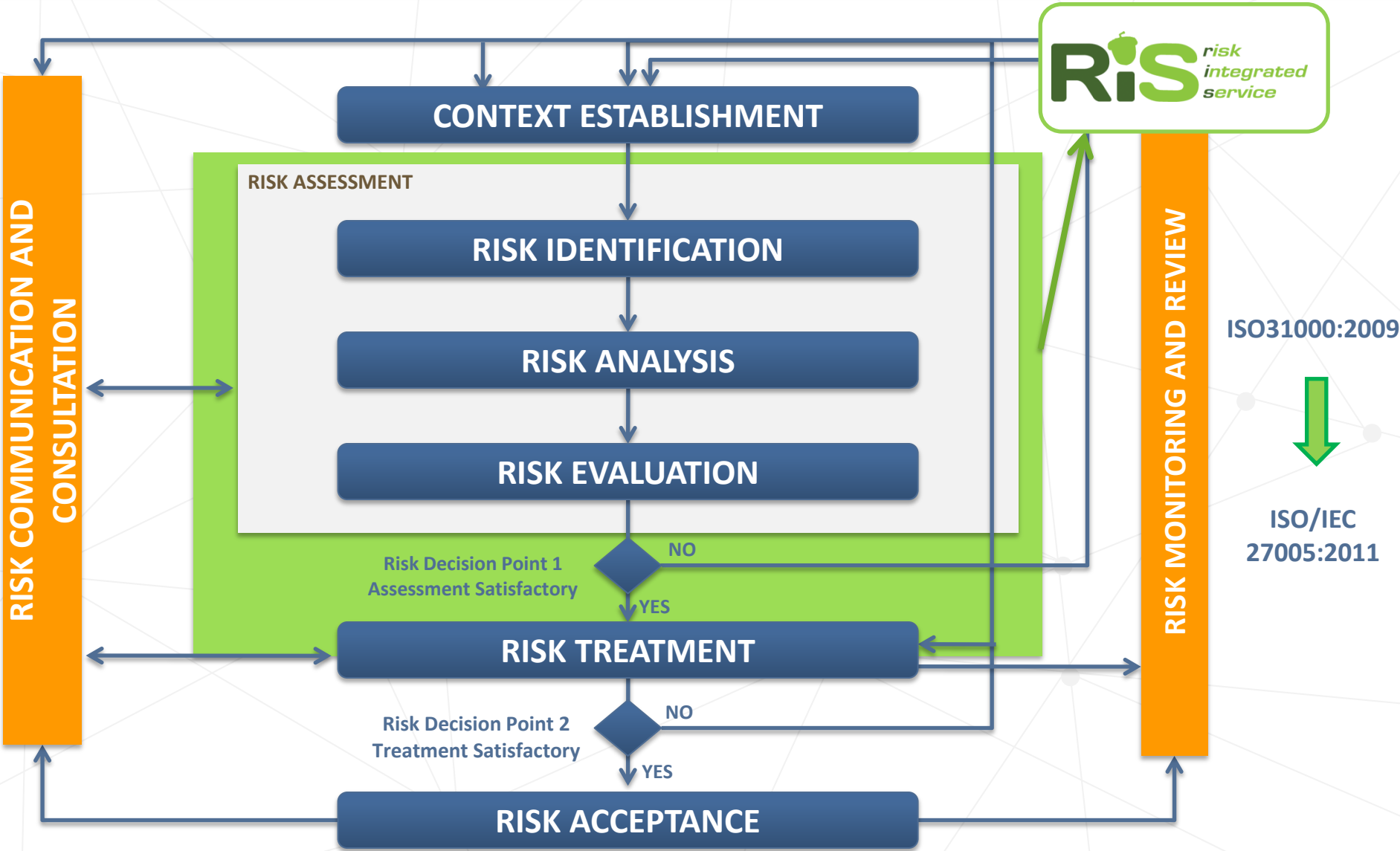
Advisory sulla Governance
dei processi di gestione dei
dati sensibili (e non)



Automatizzazione del processo
metodologico mediante
l'adozione di un tool a supporto

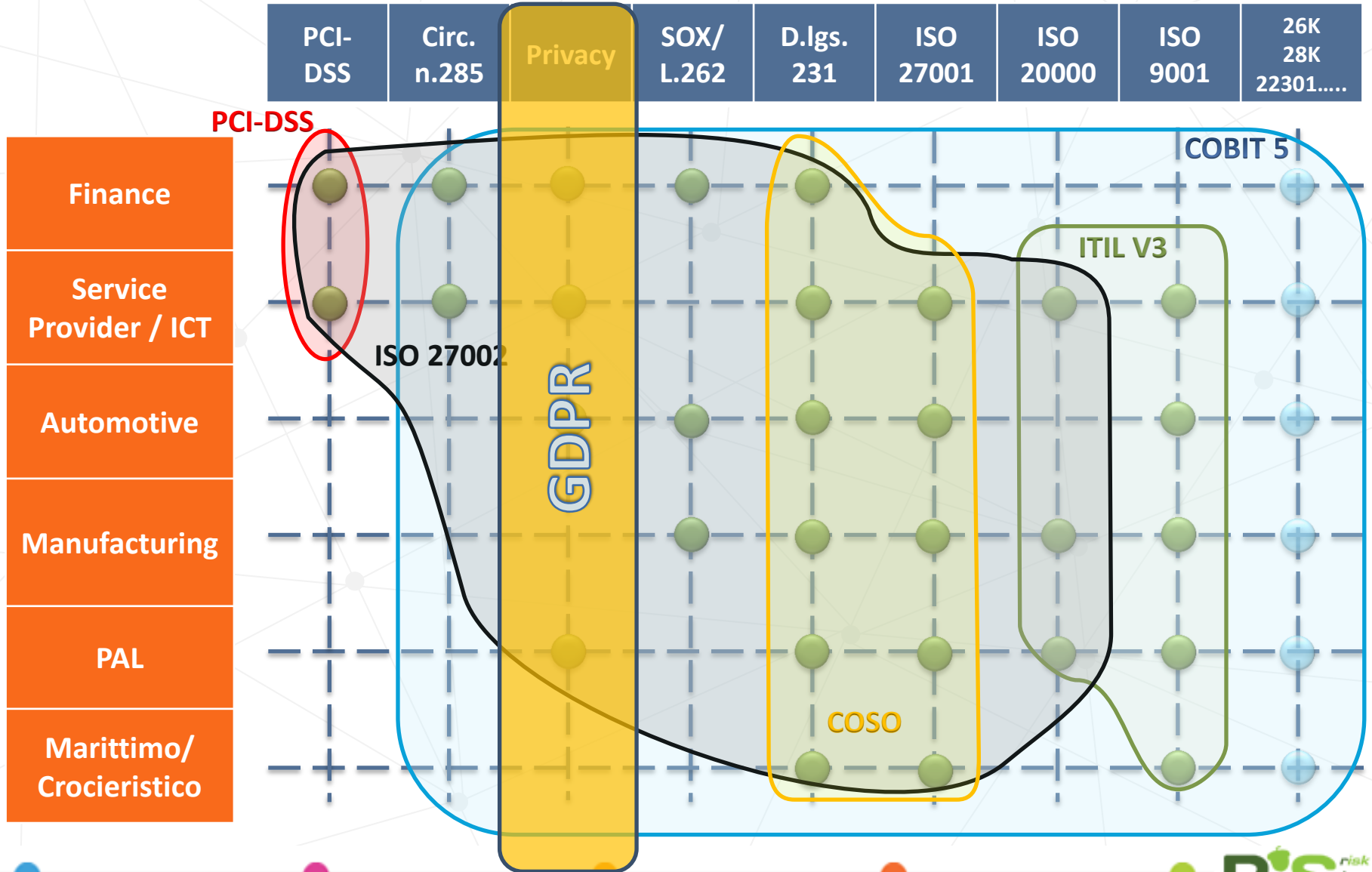
GDPR - RiS *risk
integrated
service*

Risk Management Process – ISO 31000



END OF FIRST OR SUBSEQUENT ITERATIONS

Regolamenti vs Mercato

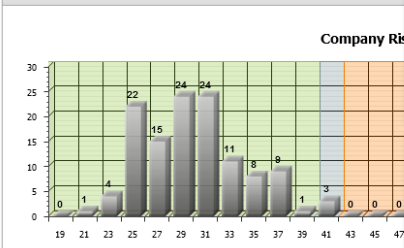


Fasi del Risk Assessment



Fasi del Risk Assessment

Risk Distribution



Asset Risk Sheet

Asset: Sala CED Genova Class: Data Processing Center
Critical Value: Very-High Risk Value: 41

Threat	Control	Applicability	Subprocess
Unauthorized Access to Physical Areas	A.11.1.3	62%	DELIVERY - Progettazione

Asset Risk Sheet

Asset: Sala TELCO GE Class: Technical Rooms (electrical, telecommunication)
Critical Value: Very-High Risk Value: 41

Threat	Control	Applicability	Subprocess
Unauthorized Access to Physical Areas	A.11.1.3	62%	DELIVERY - Progettazione

Assets with Risk Value = 41 [Read Only]

Status	Asset	Critical Level	Referent	Location	Category	SubCategory	Type	Tipology	Go To
	Sala CED Genova	Very-High		ufficio GENOVA	PHYSICAL ASSETS	LOCATION	Data Processing Center		
	Sala TELCO GE	Very-High	User Gsi	ufficio GENOVA	PHYSICAL ASSETS	LOCATION	Technical Rooms (electrical, telecommunication)		
	Sede Genova	Very-High		Genova	PHYSICAL ASSETS	LOCATION	Building		

Process Management

Process * Servizio Hosting (Centralizzato)

Shortname * HOSTING

Descrizione Servizi centralizzati erogati su infrastruttura presso il CED

1 of 2

SubProcesses

SubProcess	Description	SubProcess Shortname
<input type="checkbox"/>	Servizio di cloud provider centralizzato	C-Cloud
<input type="checkbox"/>	Servizio di co-location centralizzato	C-Co-locati
<input type="checkbox"/>	Servizio di connettività di rete geografica centralizzato	C-Wan
<input type="checkbox"/>	Servizio sistemistico DB e Middleware centralizzato	C-DB
<input type="checkbox"/>	Servizio di gestione della posta elettronica centralizzato	C-POSTA

EVALUATION

AND

CLASSIFICATION

Threats List

Category	Threat
Cause Tecniche	Hardware Malfunctioning
	Logic Bomb, Trap Doors
	Malware Software (Virus, Worm, Trojan, etc)
	Message Routing Problems
	Network Overload
	Storage Media Deterioration
	Utility Malfunctioning
Comportamenti Volontari	Company Software Wrongful Use
	Listening to Unauthorized Communications
	Repudiation

ASSETS AND VULNERABILITIES IDENTIFICATION

IDENTIFICATION OF RESOURCES IN SUPPORT OF THE INFORMATION

Info	Asset	Class	Description	Location	Asset Owner	Archiver	Level	Linked
	Access point rete corsi - wifi	Network equipment	Access Point rete wifi corsi	DMZ corsi	MANGINI			
	Accordi quadro clienti	Contracts (customer/supplier)	contratti con i clienti	DMZ Produzione	MANGINI			
	Adempimenti Legge Lavoro	D.lgs. 81/08	Adempimenti legali		MANGINI			
	Adempimento Privacy	D.lgs. 196/03	Adempimenti legali		MANGINI			
	Anagrafica Clienti	Customers database	anagrafica clienti	DMZ Produzione	MANGINI			
	Anagrafica Fornitori	Suppliers database	elenco e anagrafica dei fornitori	DMZ Produzione	MANGINI			
	Anagrafica dipendenti	Employees database	anagrafica dei dipendenti aziendali	DMZ Produzione	MANGINI			

GDPR-RIS

GDPR - RiS risk integrated service

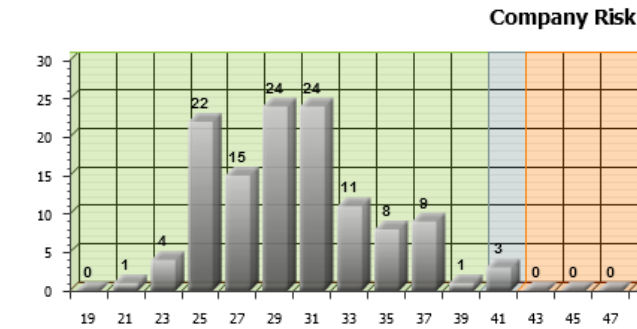
Comp

Assets over Acceptable Risk

Categories Risk Distribution

- | View | Name |
|------|---------------------------|
| ⚠ | COMPUTER RO... |
| ⚠ | LP-MANAGEMEN... |
| ⚠ | PHY_SERVER_S... |
| ⚠ | TECHNICAL COMPETENCE |
| ⚠ | SAP_ERP |
| ⚠ | SAP_ROUTER |
| ⚠ | SAP_SOLUTION MANGER |
| ⚠ | ADMINISTRATIVE COMPETENCE |

Risk Distribution



Asset Risk Sheet

Asset: Delivery/Service Manager Class: Technical competence
 Critical Value: Very-High Risk Value: 37

Threat	Control	Applicability	Subprocess
Repetition of anomalies related to personnel mistakes	A.16.1.5	67%	DELIVERY - Progettazione
	A.8.1.3	67%	DELIVERY - Progettazione

TOTAL ASSETS OCCURRENCES: 122

Asset Risk Sheet

Asset: Sala TELCO/server DR Class: Technical Rooms (electrical, telecommunication)
 Critical Value: Medium Risk Value: 37

Threat	Control	Applicability	Subprocess
Unauthorized Access to Physical Areas	A.11.1.3	62%	DELIVERY - Progettazione

Assets with Risk Value = 37 [Read Only]

Status	Asset	Critical Level	Referent	Location	Category	SubCategory	Type	Typology	To
ⓘ	Delivery/Service Manager	Very-High		Sala Costa	PERSONNEL	RISORSE UMANE	Technical competence	📁	➡
ⓘ	Responsabile Commerciale	Very-High	Solari Massimo	Sala Direzione	PERSONNEL	RISORSE UMANE	Technical competence	📁	➡
ⓘ	Sala Direzione	Very-High		Ufficio GENOVA	PHYSICAL ASSETS	LOCATION	Operating area - Offices	📁	➡
ⓘ	Sala TELCO/server DR	Medium	User Gsi	Ufficio TO	PHYSICAL ASSETS	LOCATION	Technical Rooms (electrical, telecommunication)	📁	➡

Valutazione del Rischio



ADVISOR



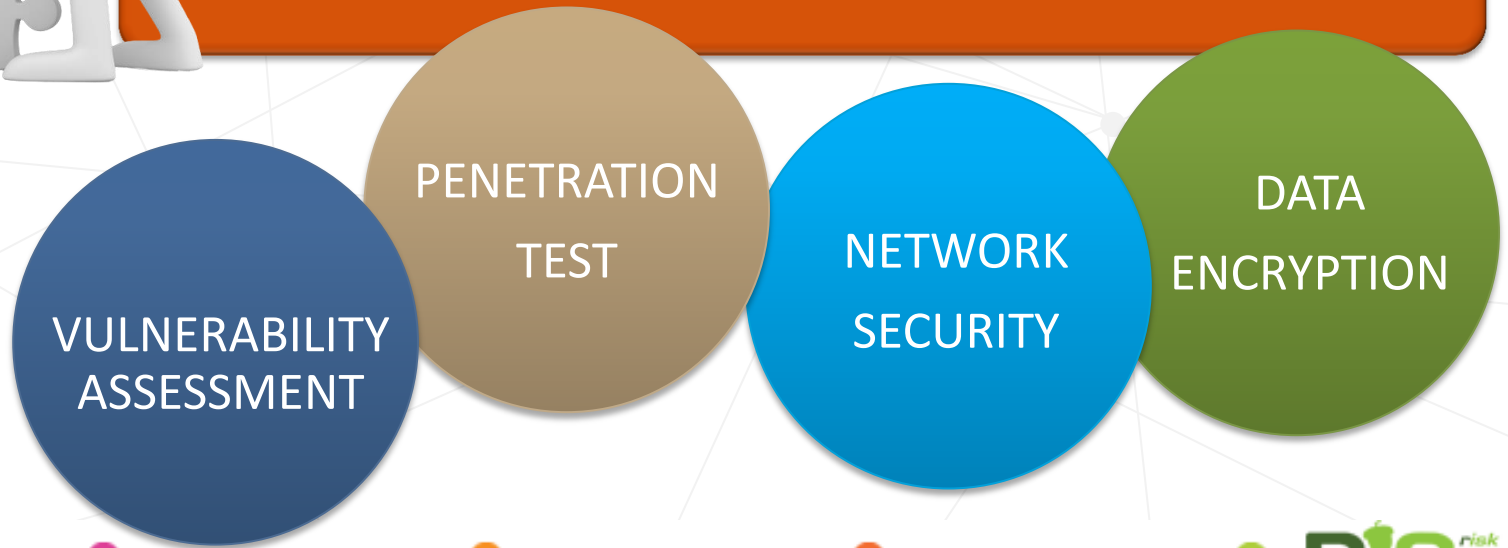
PIANO DI AZIONE



DPO



PIANO DI AZIONE



VULNERABILITY
ASSESSMENT

PENETRATION
TEST

NETWORK
SECURITY

DATA
ENCRYPTION

Grazie per l'attenzione

Alessandro Cerasoli

alessandro.cerasoli@nispro.it

Network Integration and Solutions srl

Via al Porto Antico, 7 - 16128 Genova
tel. +39 010 5954946 - fax +39 010 8680159
info@nispro.it - twitter @nis_srl

GENOVA

MILAN

TURIN

ROME