Ordine dei Dottori Commercialisti e degli Esperti Contabili di Torino

Ordine degli Avvocati di Torino

Ordine degli Ingegneri della Provincia di Torino

Tavolo di lavoro congiunto "Protezione dei dati personali – GDPR"

Checklist di base per prepararsi al regolamento generale sulla protezione dei dati

riepilogo schematico per gli studi professionali

a cura del Referente del TdL congiunto «Protezione dei dati personali – GDPR»
Ordine degli Ingegneri della Provincia di Torino

Paolo Traversa *Ingegnere*

Torino, 12 marzo 2018

Agenda

- GDPR – impegno dell'Ordine Ingegneri
- Pericoli nel mondo informatico
- GDPR - Valutazione di impatto
- *Use case*

Attività Ordine degli Ingegneri Torino/ FOIT

Data	Evento
15 luglio 2017	Seminario «Cybersecurity e Privacy 2.0»
22 Settembre 2017	Convegno «GDPR: quale impatto per le imprese»
Dicembre 2017 -	Partecipazione al tavolo di lavoro congiunto con Ordini Commercialisti e Avvocati
Febbraio-marzo 2018	Corso di aggiornamento sul GDPR (20 ore)
Febbraio 2018	Commissione Organizzazione Direzione qualità ha costituito gruppo di lavoro Privacy

General Data Protection Regulation
Dura lex … : ma da dove deriva?

Evoluzione tecnologica

- Internet
- Telefonia
- Portable devices
- Sempre connessi

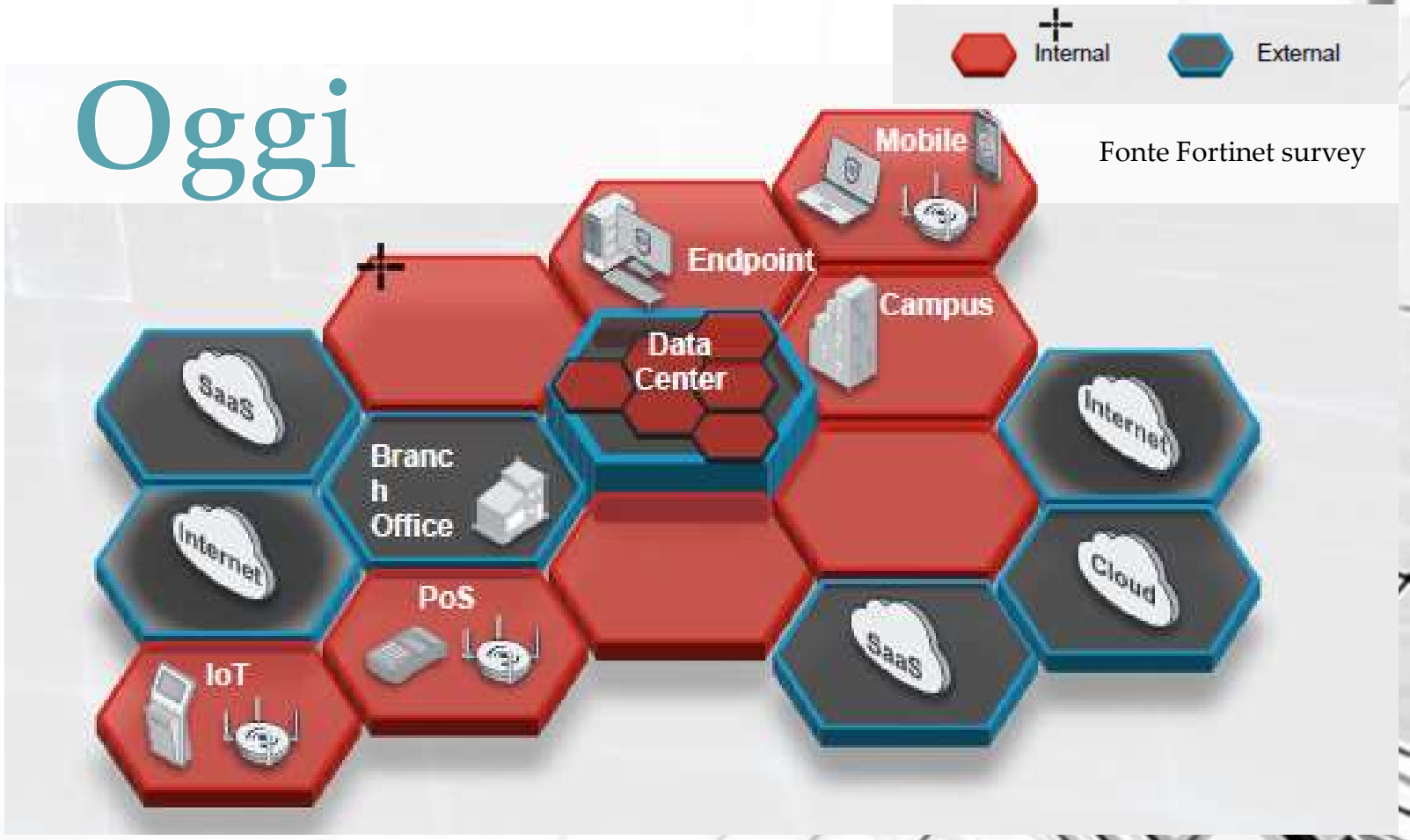
Evoluzione dei modelli di comportamento

- Condivisione
- Visibilità sui new media
- Maggiore sensibilità

Cambio del modello di sicurezza

Ieri

Oggi



Fonte Fortinet survey

Tipologie di attacco informatico: Furto di identità

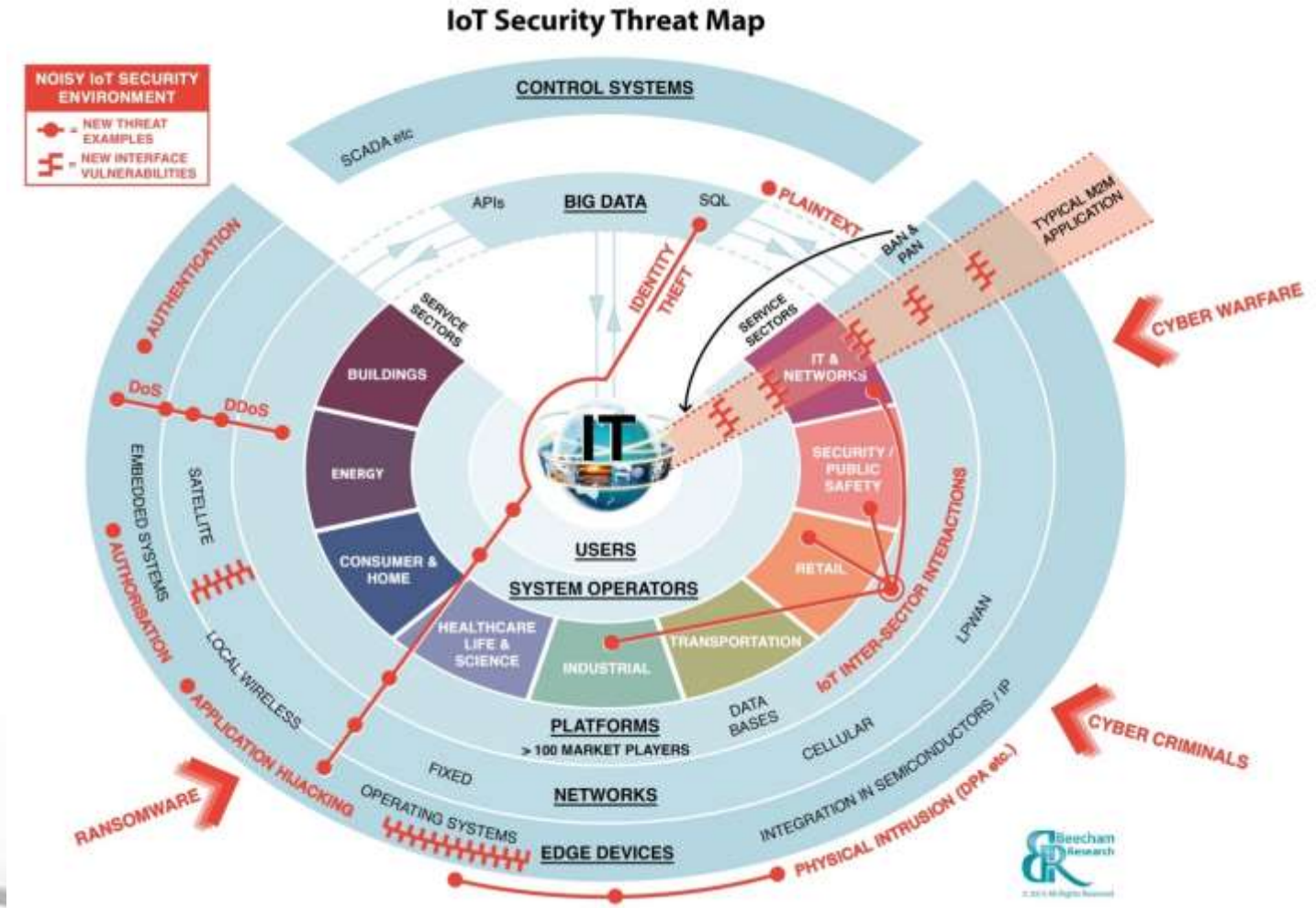
Utilizzo di credenziali altrui per:

Type of identity theft fraud	Percent
Government documents or benefits fraud	49.2%
Credit card fraud	15.8
Phone or utilities fraud	9.9
Bank fraud (2)	5.9
Attempted identity theft	3.7
Loan fraud	3.5
Employment-related fraud	3.3
Other identity theft	19.2

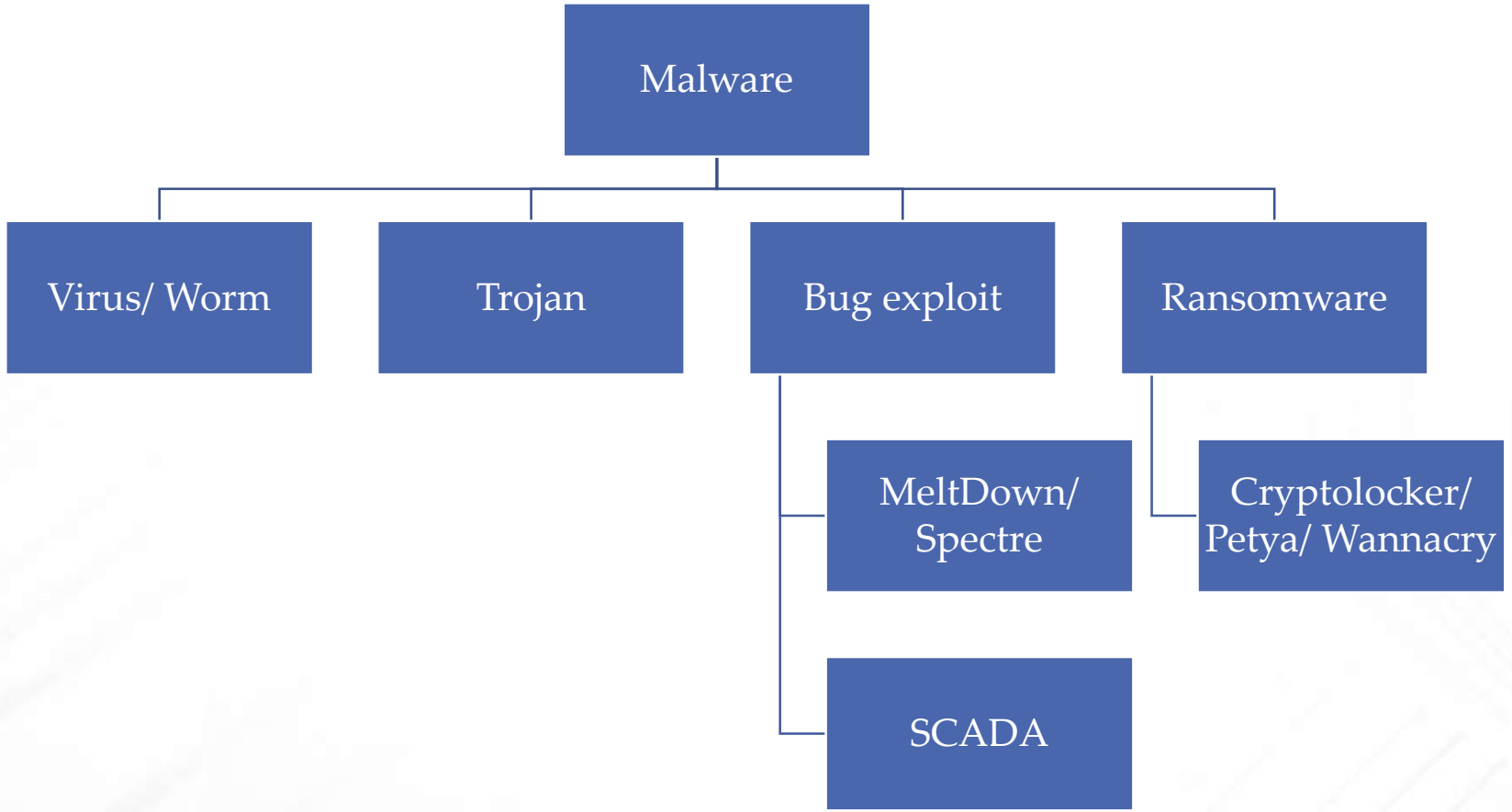
Fonte Source: Federal Trade Commission, Consumer Sentinel Network

Dati rubati da:
_ social media
_ phishing
_ grosse banche dati utente (es Yahoo/ Wind)

Tipologie di attacco informatico: IOT – Fabbrica 4.0



Tipologie di attacco informatico: Ransomware, Malware, …



Quindi da dove partire?

Art 35 GDPR: Valutazione di impatto (Data Protection Impact Analysis, DPIA)

- Obbligatoria in alcuni casi
- *Caldamente* consigliata in tutti gli altri

Come condurre una DPIA?

- Standard di analisi dei rischi
- …

Valutazione di impatto (Art 35 GDPR)

Cosa è?	• Procedura per valutare necessità e proporzionalità di un trattamento
Perché?	• la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali. (WP 29 suggerisce di attuarla su TUTTI i trattamenti e non solo dove obbligatorio)
Quando?	• PRIMA di procedere al trattamento • RIESAME CONTINUO a intervalli regolari
CHI?	• La responsabilità è SEMPRE del Titolare • DPO collabora • CSO/ CIO vengono consultati (se trattamento di tipo informatico)

Quando è obbligatoria la DPIA? (1/2)

- Trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Ad esempio:
  - trattamenti valutativi o di scoring, compresa la profilazione;
  - decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
  - monitoraggio sistematico (es: videosorveglianza);
  - trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
  - trattamenti di dati personali su larga scala;
  - %

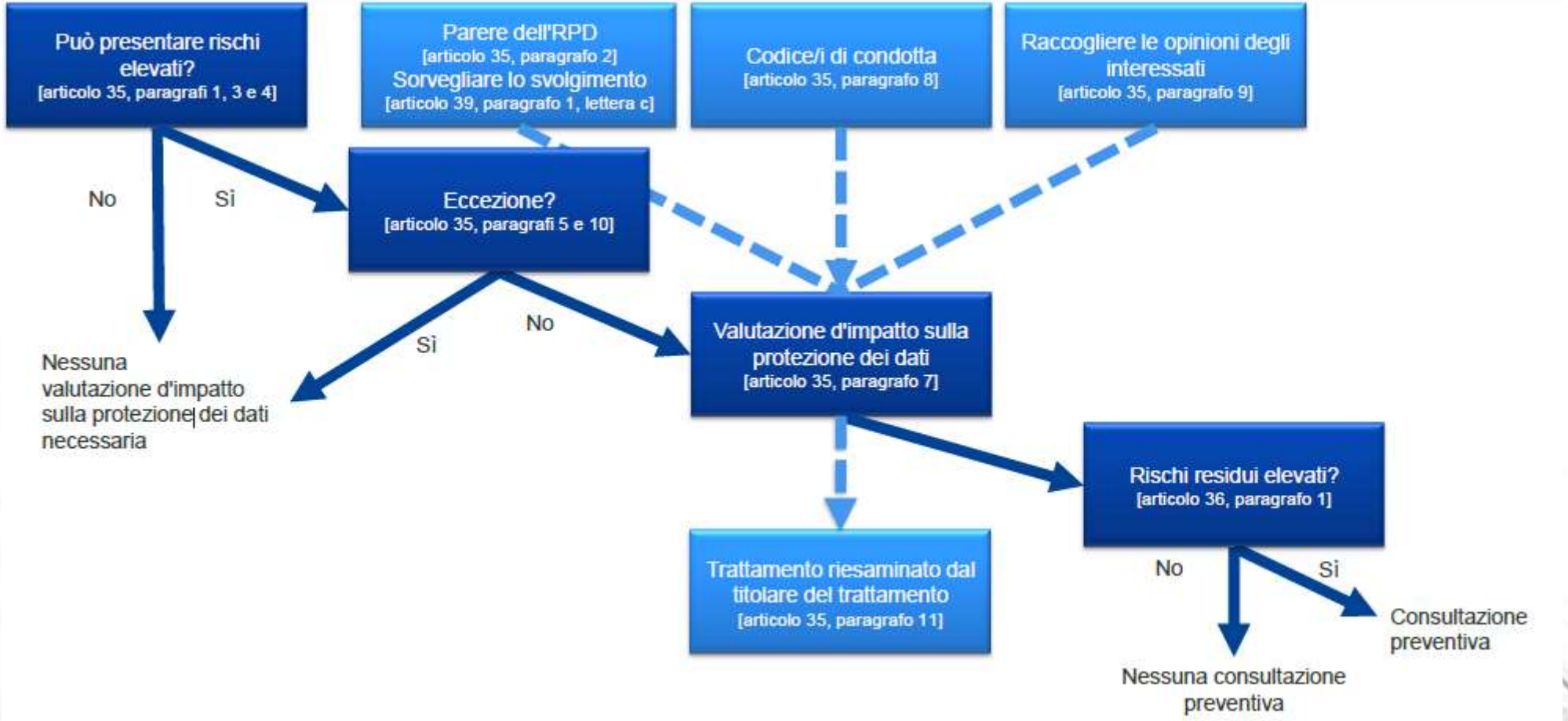
Quando è obbligatoria la DPIA? (2/2)

- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento)

Quando NON è obbligatoria la DPIA?

- Per quei trattamenti che:
  - non presentano rischio elevato per diritti e libertà delle persone fisiche; - hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
  - sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
  - sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
  - fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

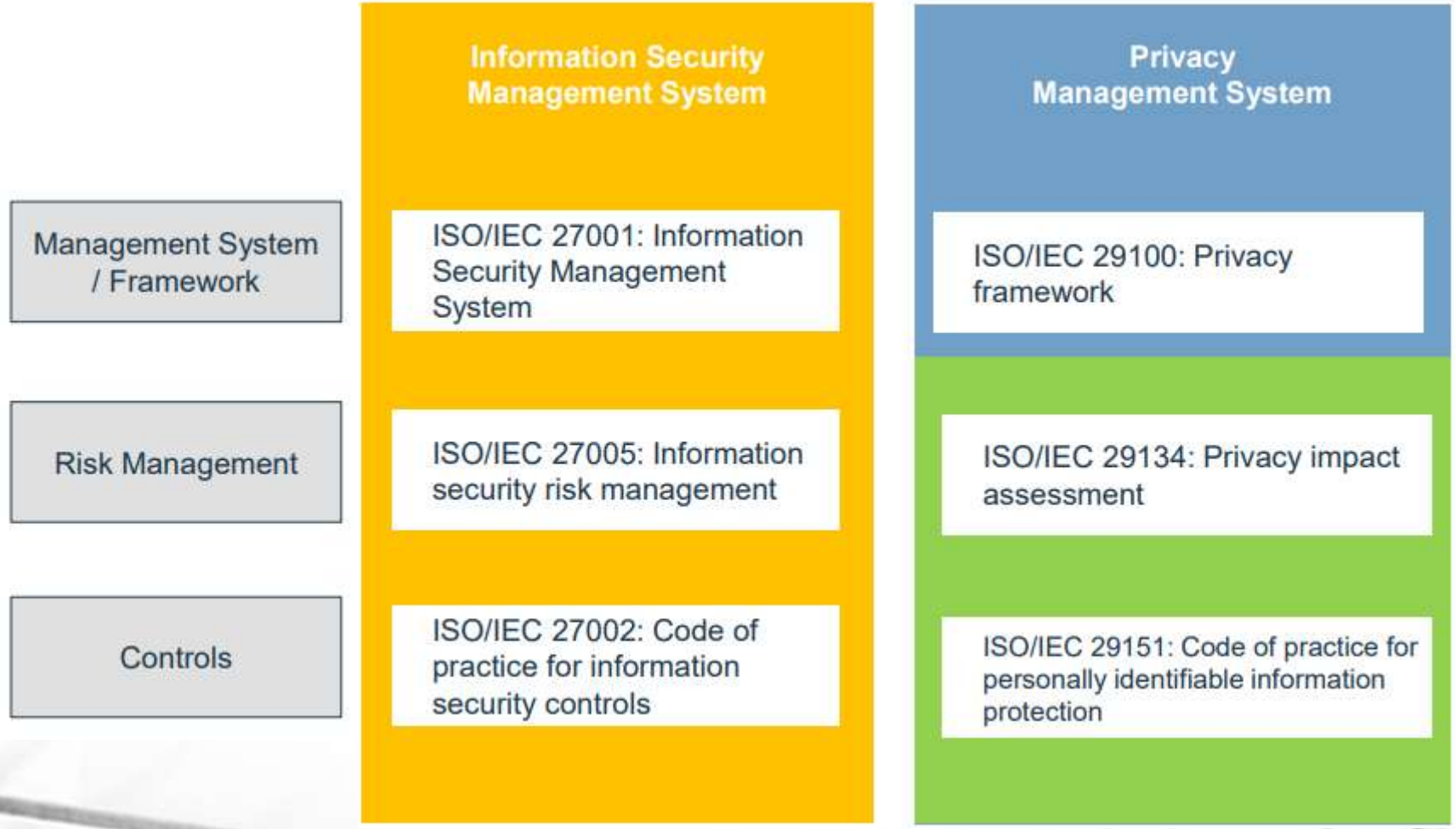
Valutazione di impatto (Linee guida da gruppo di lavoro Art. 29 WP 248)



Contenuti della DPIA (art 35, par 7)

- Descrizione dei trattamenti e delle finalità
- Valutazione necessità e proporzionalità
- Valutazione dei rischi per i diritti e le libertà degli interessati
- Misure previste per affrontare i rischi

Un aiuto dagli standard (facendo molta attenzione…)



Fonte IBM

Quale schema di certificazione è valido per GDPR?

- Ad oggi….

Misure tecniche

Pseudonomizzazione / Cifratura dei dati	
Capacità di assicurare	• Riservatezza • Integrità • Disponibilità • Resilienza
Capacità di ripristinare tempestivamente a fronte di incidenti	
Procedure per verificare regolarmente l'efficacia delle misure	

Casistica per gli Ingegneri

- CTU
- Responsabili della sicurezza
- Piccoli studi di progettazione
- Dati su contenziosi
- Progettazione che coinvolga disabili

Come ne usciamo?

- Con un po' di buon senso e tanta buona volontà
- Le *Best Practices* degli standard indicati nelle slide precedenti saranno sicuramente la base (…ma vedi i commenti delle slide precedenti)
- Al 25 maggio è FONDAMENTALE avere (almeno) INIZIATO un cammino di adeguamento e poterlo DIMOSTRARE