Misure tecniche organizzative all'interno dell'azienda, "data protection by design" e "data protection by default"

Prof. Ing. Claudio Cilli,

CIA, CISA, CRISC, CISSP, CISM, CGEIT, CSSLP, HCISPP, M.Inst.ISP

cilli@di.uniroma1.it

SAPIENZA
UNIVERSITÀ DI ROMA

Corsi e ricorsi storici

Garante per la protezione dei dati personali

Roma, li 12/04/2002
Prot. n. h398/13214

Azienda Trasporti
Milanesi S.p.A.
Foro Buonaparte, 61
20121 MILANO

Sig. Claudio Cilli
Via Berna, 25
00144 ROMA

Allegati n. 1

Oggetto: ricorso presentato dal sig. Cilli ai sensi dell'art. 29 della legge n. 675/1996.

Con riferimento al ricorso in oggetto, si trasmette copia del provvedimento adottato dal Garante per la protezione dei dati personali.

IL SEGRETARIO GENERALE
(dr. Giovanni Buttarelli)

- Un tempo esisteva la legge originale sulla privacy, la 675/96…
  - La Legge, sebbene affetta da alcuni difetti di gioventù era efficace e completa
  - L'Ufficio del garante aveva i poteri necessari e funzionava bene
  - Le sanzioni per chi la violava erano rapidamente comminate

SAPIENZA
UNIVERSITÀ DI ROMA

Corsi e ricorsi storici

- Il Documento Programmatico sulla Sicurezza (DPS) faceva più paura di una tigre affamata…
- Abusare dei dati personali raccolti era veramente difficile…
- Schiere di consulenti che neppure sapevano di quanti articoli si componeva la legge prosperavano...

SAPIENZA UNIVERSITÀ DI ROMA

La reazione delle lobby

- Era evidente che questa situazione, che vedeva il cittadino (“soggetto interessato”) al centro non poteva durare
- Le varie lobby iniziarono subito ad organizzarsi e a fare pressioni sul legislatore che alla fine, dopo un’onorevole resistenza durata quasi dieci anni, capitolò:
  - Venne introdotto il cosiddetto “ravvedimento operoso” che potava adottare chi fosse stato colto in fragranza di reato per non aver adottato le misure minime di sicurezza
  - L’accesso all’ufficio del Garante per proporre un ricorso o denunciare un abuso divenne più difficile e oneroso per il cittadino
  - L’obbligo di redigere il famigerato DPS fu abrogato
- …con il risultato che la profilazione di noi consumatori, l’inondazione di email pubblicitarie, le continue chiamate da gentili operatrici straniere dei vari call-center che sanno tutto di noi per proporci di cambiare gestore telefonico o vendere abbonamenti e servizi non richiesti e di cui non abbiamo assolutamente bisogno ci rende la vita un inferno, peggio di quando la legge sulla privacy non c’era!

SAPIENZA UNIVERSITÀ DI ROMA

Il ciclo si ripete

- L'Unione Europea, dopo un periodo di studio durato anni, caratterizzato da notizie e anticipazioni – il più delle volete inesatte e contraddittorie – bozze e versioni preliminari in circolazione ha finalmente emanato il
- GDPR (General Data Protection Regulation), normativa complessa e articolata dove, proprio come nella 679/96, è confermato il **ruolo centrale del cittdino**

SAPIENZA UNIVERSITÀ DI ROMA

Panoramica storica

- A partire dal 2012 la Commissione Europea ha proposto al Parlamento ed al Consiglio Europeo una profonda revisione ed aggiornamento della normativa privacy europea
- Il primo fondamentale obiettivo raggiunto – approvato dal Parlamento Europeo il 14 Aprile 2016 – è il Pacchetto di norme costituito da:
  - Il Regolamento Privacy Europeo per la protezione degli individui con riferimento al trattamento dei loro dati personali e relativo libero flusso nella UE (abroga e sostituisce la Direttiva Privacy 95/46/EC)
  - La Direttiva privacy specifica per regolare la protezione dei dati personali da parte delle autorità competenti a fini di prevenzione, ricerca, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati (in luogo della precedente apposita 'Framework Decision 2008/977/JHA')

SAPIENZA UNIVERSITÀ DI ROMA

Entrata in vigore del regolamento

- Approvazione ufficiale del Parlamento il 14 Aprile 2016
- Regolamento n. 2016/679 pubblicato in GUCE n. 119 del 4 maggio 2016
- Entrata in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale UE
- Effettiva applicazione a decorrere da **due anni** dalla sua entrata in vigore
- Nonostante il Regolamento generale non sia da recepire con normative nazionali, ci saranno diversi aspetti che dovranno essere disciplinati dall'Autorità Garante nazionale
- Verosimilmente, il Garante dovrà, per ognuno dei Provvedimenti e Linee Guide di carattere generale emessi fino ad oggi, valutarne la "coerenza complessiva" e la conformità rispetto al Regolamento, dovendo quindi decidere se modificarli ovvero dichiararli non applicabili

Due anni dal 14/4/2016 per l'effettiva applicazione. Non serve farsi travolgere di nuovo da consulenti agguerriti

SAPIENZA UNIVERSITÀ DI ROMA

Alcuni elementi essenziali

- La Direttiva 95/46/CE costituisce il primo corpo normativo che a livello comunitario è stato adottato per garantire la protezione dei dati personali, da cui sono scaturite le nostre leggi in materia (675/96 e 196/2003)
- Direttiva e non Regolamento perché vi era una grossa disomogeneità tra i diversi paesi aderenti molti dei quali non avevano ancora nessuna norma specifica nel proprio ordinamento destinata a garantire la protezione dei dati personali e quindi si lasciarono più ampi margini al legislatore nazionale

	Direttiva 95/46	**Regolamento sulla protezione dei dati personali**
CONSENSO	possibile sia regime di opt-in che opt-out quindi anche forme "implicite"	È necessario che vi sia un forma "esplicita" ed inequivocabile
NOTIFICAZIONE	previsto l'obbligo di notificare alcune tipologie di trattamenti	Nessun obbligo; tutto demandato alla accountability ed alla PIA
TIPOLOGIE DEI DATI	personali sensibili giudiziari	I dati Sensibili diventano "Particolari"; Viene introdotta la definizione dei dati: **genetici;** **biometrici;** **pseudo-anonimi**;
DIRITTI DELL'INTERESSATO	conferma del trattamento, accesso ai dati, rettifica,cancellazione, limitazione e/opposizione per determinate finalità o operazioni di trattamento	**Diritto all'oblio;** **Diritto alla portabilità dei dati;**

PIA = Privacy Impact Assessment

SAPIENZA UNIVERSITÀ DI ROMA

Panoramica storica

- La normativa europea specifica alcuni elementi espressi in termini prima generici di interesse per questa presentazione:
  - **Gestione accountability**: attestazione documentata degli adempimenti privacy presi in carico; controllo sui trattamenti effettuati, responsabilità e compiti assegnati, misure di sicurezza implementate
  - **Gestione Data Breach**: definizione ed implementazione di piani di gestione e relativa organizzazione e test, utilizzo di strutture informative per documentare gli eventi di Data Breach, organizzazione e mezzi per rispettare le tempistiche di legge
  - **PIA**: Definizione ed implementazione di metodi per condurre, documentare e gestire nel tempo le attività di PIA ed eventuali conseguenti *Prior Consultation* con il Garante Privacy

- Oltre alla ridefinizione di alcune figure specifiche

	Direttiva 95/46	**Regolamento sulla protezione dei dati personali**
TITOLARE DEL TRATTAMENTO	Definizione e ambiti di responsabilità descritti in forma molto light	Indicati gli oneri connessi alla titolarità: Privacy by design e by default; Misure idonee in relazione ai trattamenti; Autonoma valutazione dei rischi (PIA); Documentazione dei trattamenti e self assessment periodico di verifica.
RESPONSABILE DEL TRATTAMENTO	Definizione e ambiti di responsabilità descritti in forma INDIRETTA	Accountability diretta del Responsabile anche in ordine al risarcimento del danno; Contratto o altro atto giuridico per regolare i rapporti con il Titolare; Possibile impiego di sub-fornitori con delega del Titolare.
DATA PROTECTION OFFICER	Figura non prevista	Obbligatorio per la PA e in caso di monitoraggio regolare e sistematico su larga scala e trattamento su larga scala di dati sensibili e giudiziari; "suggerito" per gli altri Titolari in quanto figura che svolge un ruolo di cerniera nei confronti della Autorità; Esperto di protezione dati sia per gli aspetti legali che tecnici. Dipendente o Consulente con ampi margini di autonomia

SAPIENZA UNIVERSITÀ DI ROMA

Privacy by Design and by Default

"Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"

- **By Design**
  - Sia in fase di determinazione dei mezzi di trattamento sia nel corso del trattamento il Titolare adotta adeguate misure tecniche/organizzative/procedurali (citata come esempio la pseudoanonimizzazione) per soddisfare principi e requisiti del GDPR, incluso il rispetto dei diritti degli Interessati

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento,

- **By Default**

- Come pre-impostazione il Titolare adotta adeguate misure tecniche/organizzative/procedurali, tali che, siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento, in termini di:
  - quantità dei dati personali raccolti,
  - l'estensione del loro trattamento,
  - il periodo di conservazione e l'accessibilità
- L'adesione ad un sistema di certificazione privacy autorizzato come da GDPR può essere utilizzato per dimostrare la conformità ai requisiti Privacy By Design e By Default (art. 25)

SAPIENZA UNIVERSITÀ DI ROMA

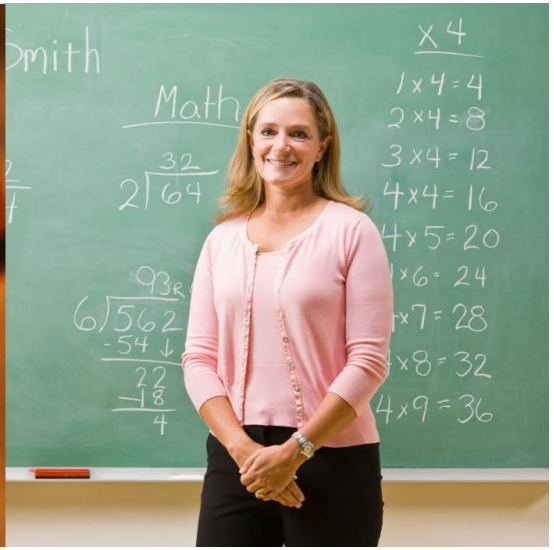
A proposito di certificazioni…

- *Art. 39 Comma 1: "Gli Stati membri, le autorità di controllo, il comitato europeo per la protezione dei dati e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai responsabili del trattamento e dagli incaricati del trattamento. Si tiene conto delle esigenze specifiche delle micro, piccole e medie imprese."*
- *Art. 39 Comma 1ter: "La certificazione è volontaria e accessibile tramite una procedura trasparente."*
- *Art. 39 Comma 2. "La certificazione ai sensi del presente articolo non riduce la responsabilità del responsabile del trattamento o dell'incaricato del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri dell'autorità di controllo competente a norma degli articoli 51 o 51 bis."*

Come per tutte le certificazioni, anche quando l'infrastruttura accreditata sarà disponibile, le conseguenze di un trattamento illecito dei dati non sono ridotte o trasferite ad altri soggetti anche se il proprio sistema di gestione della privacy, o le figure responsabili ("**Data Protection Officer**", ecc.) hanno ottenuto delle certificazioni.

SAPIENZA UNIVERSITÀ DI ROMA

Privacy Impact Assessment



Chi possiede i dati?

Chi controlla i dati?

Chi elabora i dati?

SAPIENZA
UNIVERSITÀ DI ROMA

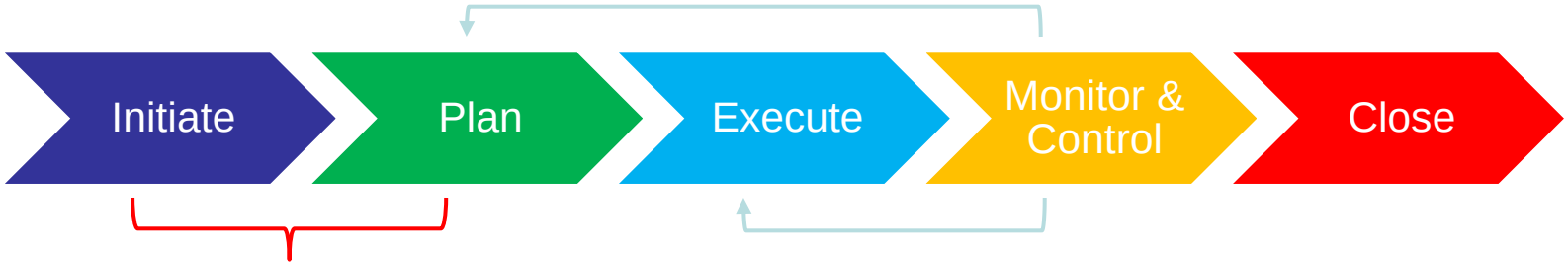
Privacy Impact Assessment

- Metodologia utilizzata per verificare se un nuovo progetto:
  - ha rischi potenziali per la privacy
  - la severità di questi rischi e
  - ogni azione che può essere intrapresa per eliminare o mitigare questi rischi

- Integrata o compresa nel risk assessment

SAPIENZA UNIVERSITÀ DI ROMA

Privacy By Design



PIA Initiation
- Define scope of PIA
- Designate team resources
- Adapt PIA to reflect scope

Data Analysis
- Conduct interviews
- Identify information flow and personal information types

Privacy Analysis
- Consult with stakeholders
- Legal/regulatory compliance
- Document privacy issues and implications

PIA Report
- Summarise privacy risks and risk levels
- Identify and explore remedial options
- Submit report

SAPIENZA UNIVERSITÀ DI ROMA

Off-the-shelf software

- Verifiche essenziali

Activity	Potential Privacy Risk	Harm to Client	Harm to Org.	Remedial options
Contacting clients by email for promotional purposes. Current promotional contact by post.	May be used in ways that are unacceptable/ unexpected by the data subject	Annoyance (low privacy risk)	Loss of custom /client	Written consent Future consent via customer registration form Manage frequency of communication through -policy/training? -restrict access to mass mailing?

SAPIENZA UNIVERSITÀ DI ROMA

Possibili rimedi

- Controlli tecnologici
  - Controllo accessi
  - Monitoraggio delle Email e della rete
  - Business continuity - Backup ‘in the Cloud’
  - Smaltimento sicuro degli hard-disk
- Controlli organizzativi
  - Information Security / Data Protection Policy
  - Staff Training
  - Chiarezza nella definizione dei ruoli/responsabilità
  - DPO designato con almeno mezza giornata dedicata a queste tematiche

SAPIENZA UNIVERSITÀ DI ROMA

Privacy by Default

Article 23: The controller shall implement mechanisms for ensuring that, by default, only those personal data which are necessary for the purposes of the processing are processed.

- Controlli di sicurezza incorporati nei prodotti/servizi
- Privacy-friendly default settings (Hello, Facebook)
- Collaborazione con l'IT
- Necessaria attività per mettere a norma i sistemi esistenti

SAPIENZA
UNIVERSITÀ DI ROMA

È giunto il momento dell'Information Governance?

- Garantisce che le politiche sulle conservazioni siano aggiornate
- Armonizza le politiche sulla conservazione con quelle sulla privacy
- Rafforza i processi legali legati alla privacy
- Migliore gestione dei dati grazie ad una strategia di distribuzione

- Aiutando a definire la mappatura dei dati consente di sviluppare processi di cancellazione/distruzione difendibili
- Favorisce la "Cultura della Compliance" grazie all'Information Governance Behavior Change Management (cultura del cambiamento)
- Aiuta a definire Politiche e Procedure qualora il Change Management non è sufficiente

SAPIENZA UNIVERSITÀ DI ROMA

GRC

GRC:

- **Governance, Risk management e Compliance**
- Un termine sempre più utilizzato per come “ombrello” per comprendere queste tre aree dell’attività aziendale
- Queste aree di attività si stanno sempre più allineando e integrando per migliorare le performance dell’impresa e il soddisfacimento dei bisogni degli stakeholder

SAPIENZA UNIVERSITÀ DI ROMA

GRC: Definizioni

GRC:

- **Governance** — *Esercizio dell'autorità; controllo; governo; composizione*
- **Risk** (management) – *rischio; pericolo; esposizione a perdita, danno o distruzione (l'atto o l'arte di gestire; il modo di trattare, orientare, esercitare, o utilizzare, per uno scopo; comportamento; amministrazione; orientamento; controllo)*
- **Compliance** – *Il rispetto e l'osservanza della legge; una concessione, come un desiderio, domanda, o proposta; concessione; presentazione*
- Webster online dictionary

SAPIENZA UNIVERSITÀ DI ROMA

Implementare la Governance

- L’integrazione dell’implementazione delle attività di GRC all’interno di un’organizzazione richiede un approccio sistematico per raggiungere affidabilmente gli obiettivo di business dei suoi stakeholders
- Tali approcci sono basati tipicamente su abilitatori di vario tipo (es.: principi, politiche, modelli, framework, strutture organizzative)

SAPIENZA
UNIVERSITÀ DI ROMA

Corporate Governance dell'IT

ISO/IEC 38500: 2008

Corporate governance of information technology

1.1 Scopo

- Lo standard fornisce i principi guida per gli amministratori di organizzazioni (tra cui proprietari, amministratori, senior manager, soci, dirigenti, o simili) per un utilizzo in modo efficace, efficiente e accettabile delle tecnologie dell'informazione (IT) all'interno delle loro organizzazioni
- Questo standard si applica alla governance dei processi di gestione (e decisioni) relative alle informazioni e ai servizi di comunicazione utilizzati da un'organizzazione. Questi processi possono essere controllati da specialisti IT all'interno dell'organizzazione o da fornitori esterni di servizi, o per unità di business all'interno dell'organizzazione

SAPIENZA UNIVERSITÀ DI ROMA

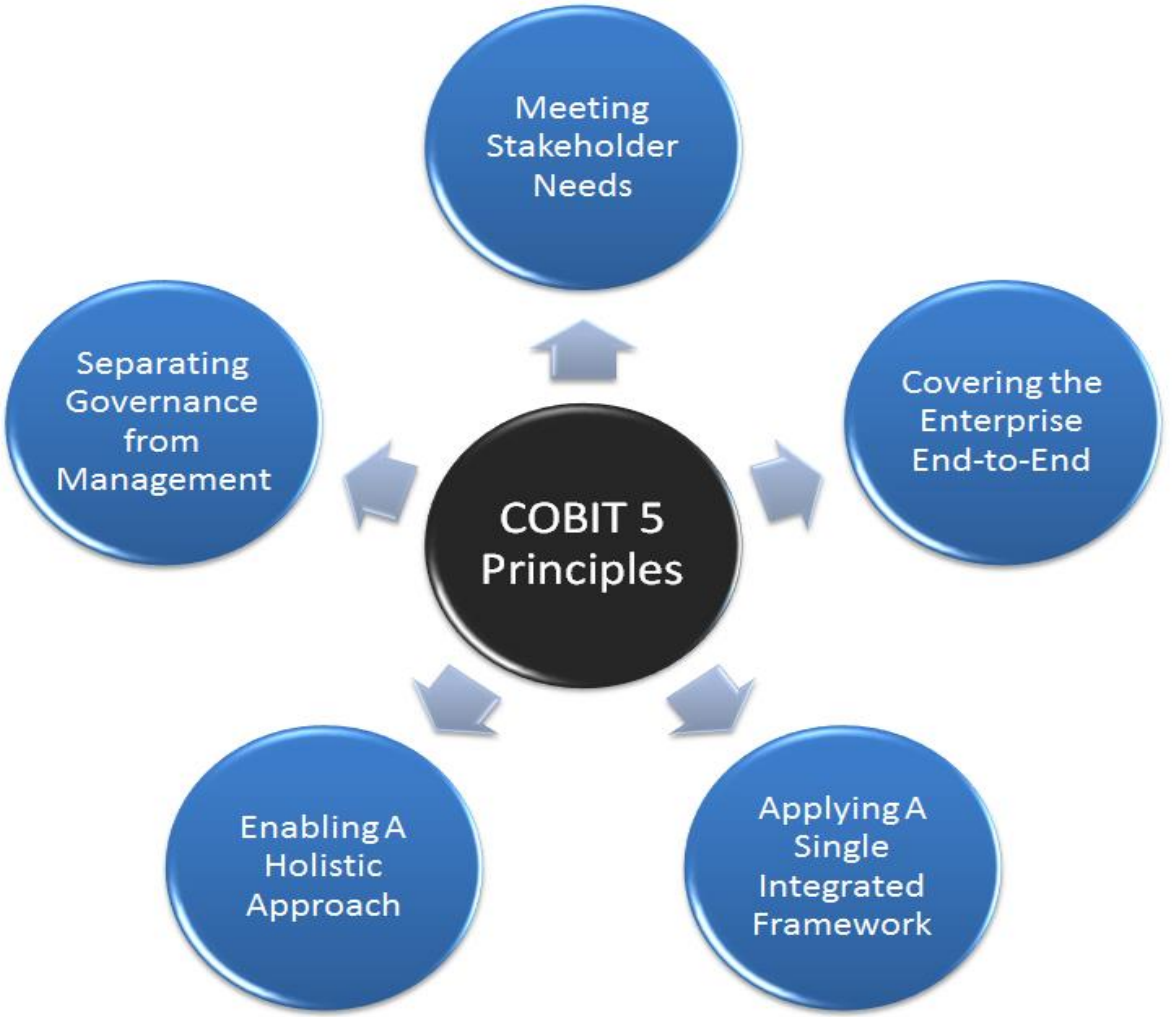
Metodologie di GRC: CObIT 5

COBIT 5

- Unisce i **cinque principi** che
- consentono all'impresa di realizzare un'efficace framework di **governance** e **management** basato su
- un insieme olistico di **sette abilitatori** che
- ottimizza le **informazioni** e gli investimenti in **tecnologia** e le utilizza a beneficio degli stakeholder

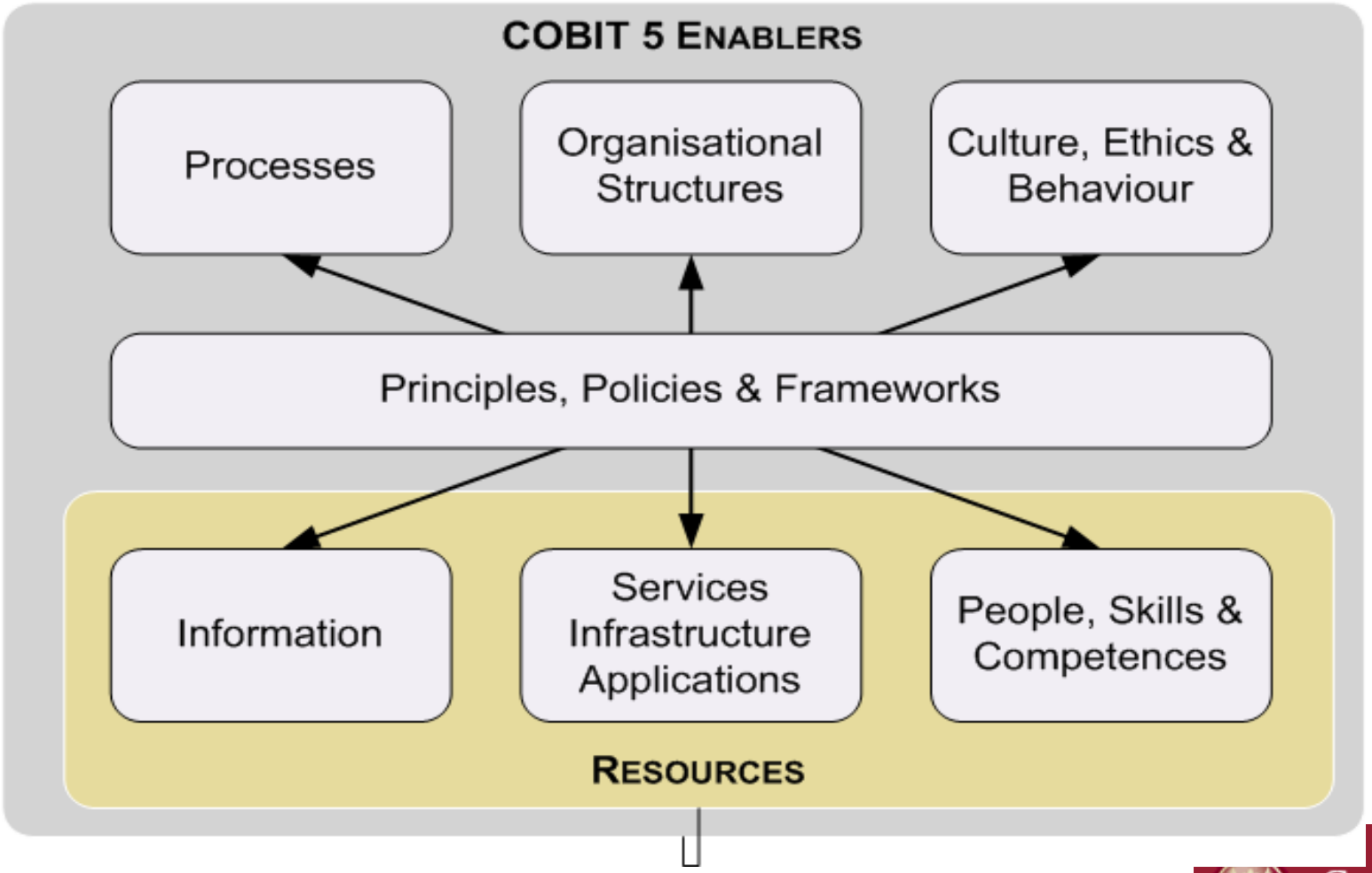
SAPIENZA
UNIVERSITÀ DI ROMA

CObIT 5: Principi



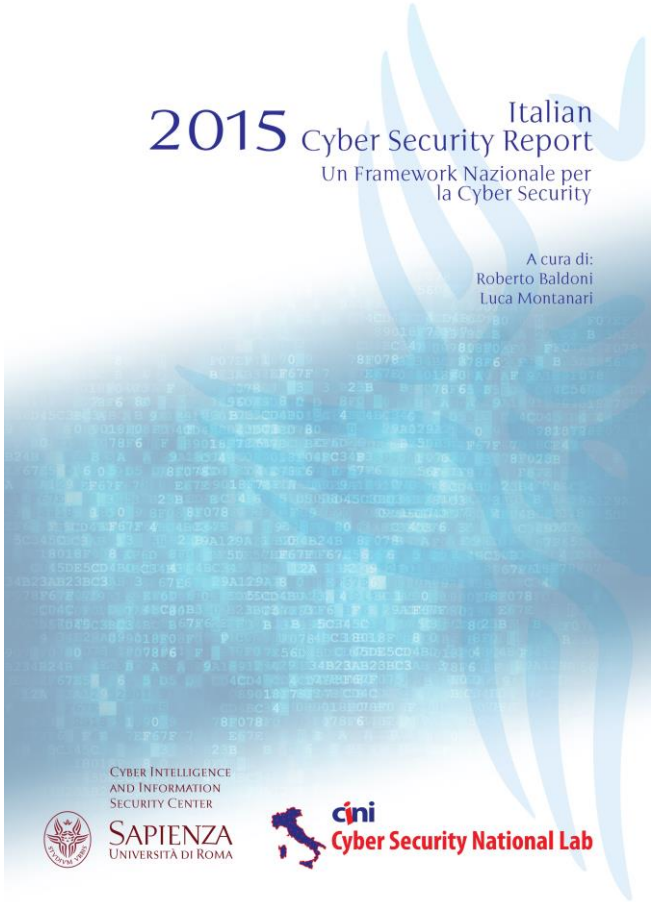
SAPIENZA UNIVERSITÀ DI ROMA

CObIT 5: Abilitatori (enablers)



SAPIENZA UNIVERSITÀ DI ROMA

Cosa fare in pratica?



- Il framework nazionale nasce da una ricerca guidata dall'Università di Roma "La Sapienza" e il National Institute for Standards and Technologies (NIST)

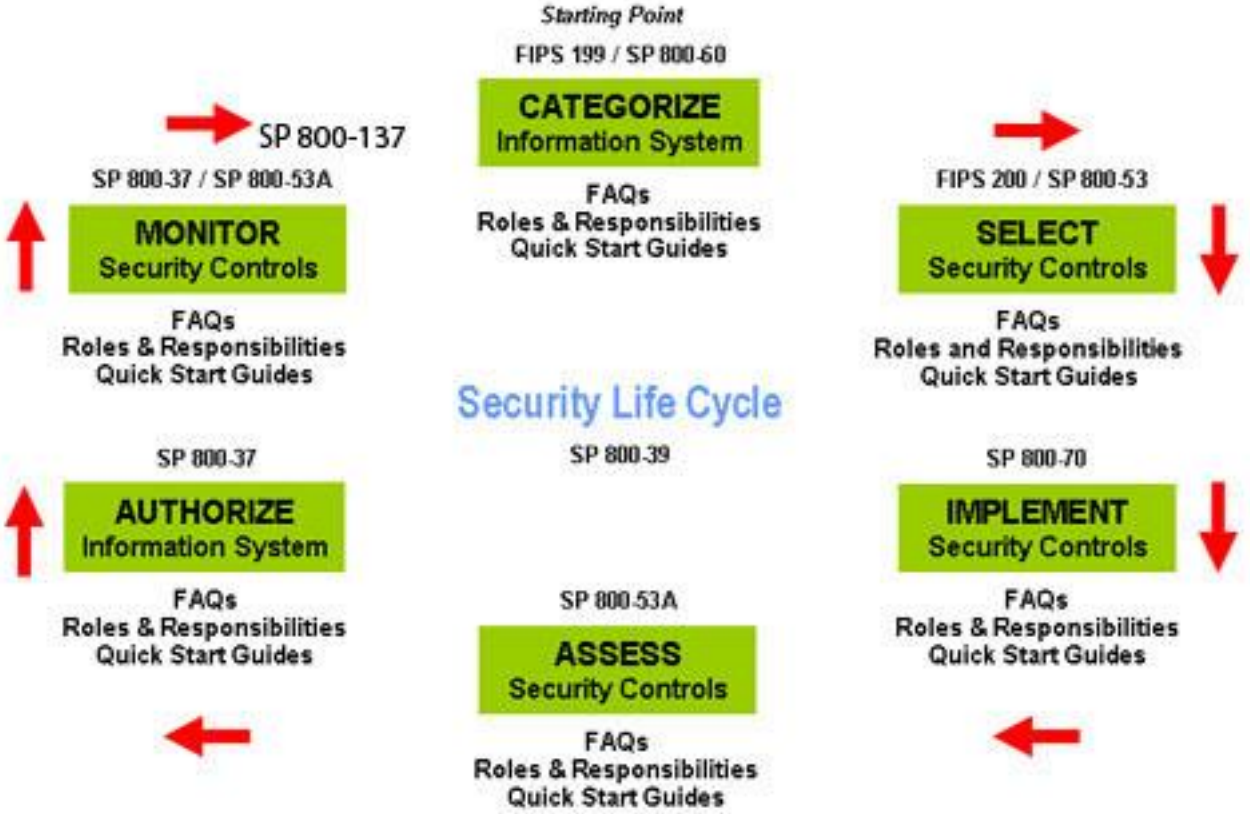
Cybersecurity framework?

- “The security professional needs to adhere to a framework.... once the security professional begins to bring order to the organization’s security program, they are implementing a framework.” -- http://www.securitycurrent.com/en/writers/david-sheidlower/security-where-myths-should-go-to-die
- Benefici:
  - Dal caos all’ordine e all’organizzazione
  - Pratiche e politiche gestibili
  - Strumenti / meccanismi → architetture / politiche → strategia / governance

SAPIENZA UNIVERSITÀ DI ROMA

Il framework NIST

National Institute of Standards and Technology
U.S. Department of Commerce



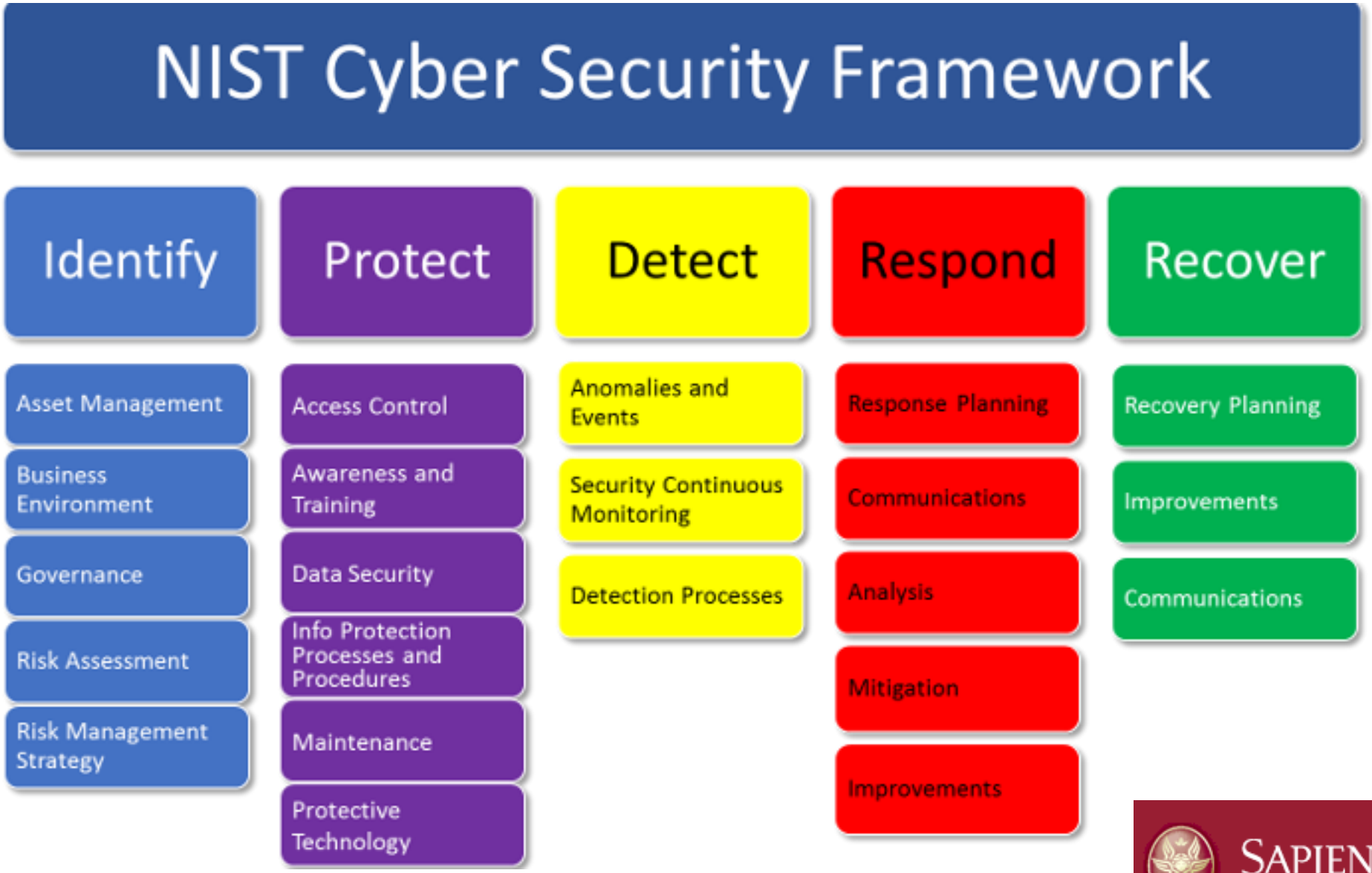
Sapienza Università di Roma

Il framework NIST

Isaca CObIT for NIST

SAPIENZA UNIVERSITÀ DI ROMA

Il Framework NIST



SAPIENZA UNIVERSITÀ DI ROMA

The NIST Framework Core

The Core is a set of cybersecurity activities, desired outcomes, and applicable references that presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level

Functions: provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk

Categories: provide a group of cybersecurity outcomes tied to programmatic needs and particular activities?

Subcategories: provides a specific activity or result mapped to a reference that helps support achievement of higher level outcomes

Informative References: provides specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve an associated outcome?

SAPIENZA UNIVERSITÀ DI ROMA

Funzioni

Identify - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Protect - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Detect - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event

Respond - Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Recover - Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

SAPIENZA UNIVERSITÀ DI ROMA

Implementazione

The Framework is risk-based, and is composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy	ID.AM-1: Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6

TIER 1
Partial

Tier 2
Risk Informed

Tier 3
Repeatable

TIER 4
Adaptive

SAPIENZA
UNIVERSITÀ DI ROMA

Grazie per l'attenzione!

SAPIENZA
UNIVERSITÀ DI ROMA