Gli strumenti di misurazione della conformità al Regolamento UE sulla protezione dei dati personali 2016/679 (GDPR)

Giancarlo Butti

EUROPRIVACY.INFO
#READY4EUDATAP

*Le affermazioni e le opinioni espresse nel presente documento **sono esclusivamente dell'Autore** e non vincolano in alcun modo le organizzazioni di appartenenza.*

Giancarlo Butti *(LA BS7799), (LA ISO IEC 27001:2013), CRISC, ISM, DPO, CBCI*

Master di II livello in Gestione aziendale e Sviluppo Organizzativo (MIP - Politecnico di Milano).

Mi occupo di ICT, organizzazione e normativa dai primi anni 80:

- analista di organizzazione, project manager, security manager ed auditor presso gruppi bancari
- consulente in ambito documentale, sicurezza, privacy… presso aziende di diversi settori e dimensioni.

Come divulgatore ho all'attivo:

- oltre 700 articoli su 20 diverse testate tradizionali e 7 on line
- 19 fra libri e white paper, alcuni dei quali utilizzati come testi universitari e 6 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT 2016
- membro della faculty di ABI Formazione, docente presso altre istituzioni e relatore presso eventi di ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF…

Socio e proboviro di AIEA/ISACA e socio del CLUSIT.

- Partecipo ai gruppi di lavoro di ABI LAB sulla Business Continuity e Rischio informatico, di ISACA-AIEA su Privacy EU e 263, di Oracle Community for Security su privacy, frodi, eidas, sicurezza dei pagamenti, di UNINFO sui profili professionali privacy, di ASSOGESTIONI su Privacy EU.
- Fra i coordinatori di www.europrivacy.info.

Approccio al GDPR

Fra le novità del nuovo Regolamento privacy il passaggio da una conformità **statica** ad una **conformità dinamica** (intervento di Isabelle Falque Pierrotin del 16 Marzo 2016)

- ad esempio non vengono definite regole precise per definire le misure di sicurezza da adottare (non esistono le misure minime di sicurezza)
- al Titolare è richiesto:
  - di pensare (e ripensare) un trattamento di dati personali in un'ottica che ne preveda una **protezione** fin dalla progettazione *(Data protection **by design** and by default nella terminologia anglossasone)*,
  - di dimostrare, e quindi **documentare** con evidenze oggettive in ogni momento (**accountability**), la propria conformità al Regolamento.

Isabelle Falque Pierrotin [*]'s speech – 16 March 2016

***First**: compliance obligations. The Regulation is a turning point for you, for the **business**: no more (or at least fewer) administrative paper work BUT more real compliance.*

*With the regulation, we go from static to **dynamic compliance**.*

*More real compliance through a wide range of tools that the company can **pick and choose** to ensure the best compliance possible.*

[*} Presidente W29

PROTEZIONE e Sicurezza

Decreto legislativo 30 giugno 2003, n. 196

Codice in materia di **PROTEZIONE** dei dati personali

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla **PROTEZIONE** delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla **PROTEZIONE** dei dati)

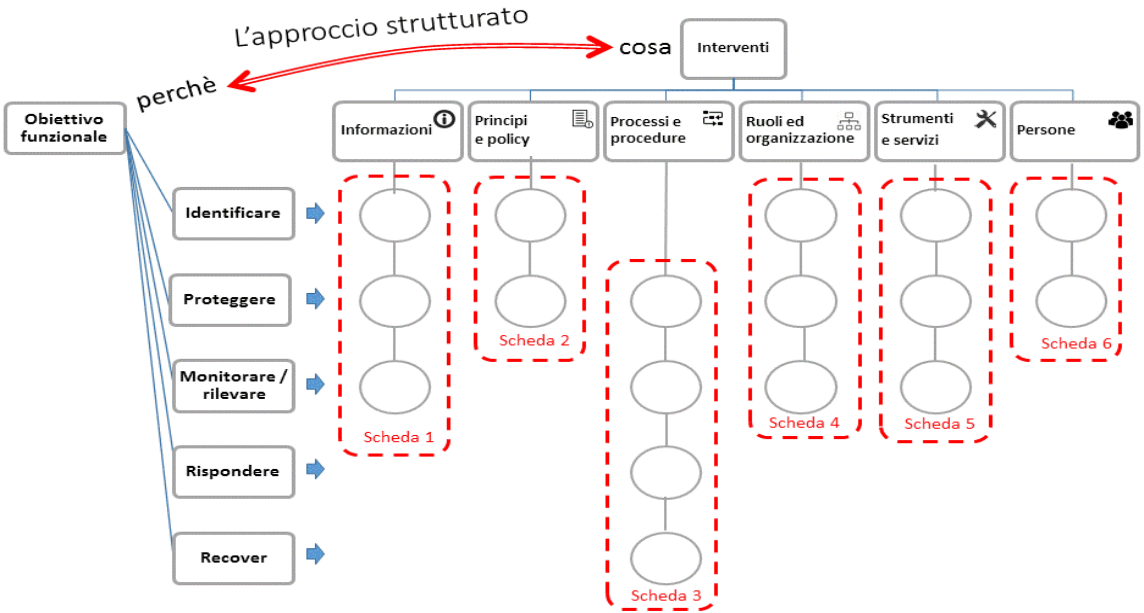
ACCOUNTABILITY

(85) …unless the controller is able to demonstrate, in accordance with the **accountability** principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

*(Art. 5) …The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (**'accountability').***

GLI STRUMENTI
per la conformità

Strumenti per implementare



Strumenti per implementare

3. Privilegiare le richieste degli interessati in base alla classificazione e urgenza.		
Procedura	Input	Output
3 - Verificare, approvare ed espletare le richieste degli interessati. Selezionare le procedure di risposta opportune verificando che le richieste soddisfino i criteri previsti. Ottenere l'approvazione, ove necessario, ed espletare le richieste.	Richiesta interessato	Richieste degli interessati approvate Richieste degli interessati respinte
		Richieste degli interessati espletate
1. Verificare l'idoneità delle richieste degli interessati, utilizzando, ove possibile, un flusso di processo		
2. Ottenere l'approvazione funzionale, ove previsto, oppure approvazioni predefinite per le richieste standard.		
3. Espletare le richieste eseguendo la procedura selezionata, utilizzando, se disponibili, strumenti automatici o modelli predefiniti.		

MISURE DI SICUREZZA DEL CED

Identificazione locale

Denominazione _____
Piano _____

- ☐ Adeguato posizionamento all'interno dell'edificio
- ☐ Pareti soffitto/pavimento
- ☐ Pareti di adeguato spessore e robustezza
- ☐ Misure anti effrazione
- ☐ Controllo accessi
- ☐ Videosorveglianza
- ☐ Rilevatori di fumo, calore, allagamento
- ☐ Misure antincendio idonee all'uso con le apparecchiature presenti
- ☐ Porte antincendio di adeguata dimensione
- ☐ Interruttore generale della alimentazione elettrica
- ☐ Impianto di climatizzazione
- ☐ .....
- ☐ .....

ARCHIVI CARTACEI (DOCUMENTI/SUPPORTI)

Identificazione locale

Denominazione _____
Piano _____

Sistema di custodia

- ☐ Armadi blindati
- ☐ Armadi ignifughi con serratura
- ☐ Armadi ignifughi senza serratura
- ☐ Altri armadi con serratura
- ☐ Altri armadi senza serratura
- ☐ Classificatori/cassetti con serratura
- ☐ Classificatori/cassetti senza serratura
- ☐ Cassaforte
- ☐ Scaffalature
- ☐ .....

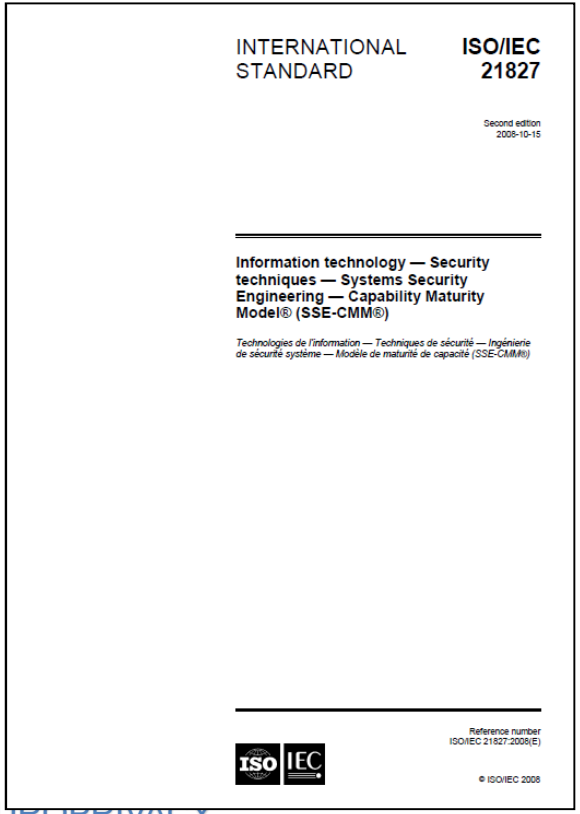
Tipo di archivio/media

- ☐ Operativo
- ☐ Storico
- ☐ Cartaceo
- ☐ Supporti ottici
- ☐ Supporti magnetici
- ☐ Microfilm
- ☐ .....

NORME DI COMPORTAMENTO - Comunicazioni

Cosa fare	Cosa non fare
Telefono	
• Fornire solo le informazioni per le quali si è stati esplicitamente autorizzati • Segnalare al proprio responsabile richieste inusuali di informazioni • Nel caso di comunicazioni in viva voce informare l'interlocutore dell'attivazione di tale modalità e della presenza di eventuali altri ascoltatori; verificare in questo caso la presenza di terzi non autorizzati	• Fo • Fo • Fo • Fo au
Segreterie telefoniche	
	• La
Cellulari	
• Utilizzare password di accesso per la protezione della rubrica e dei dati • Bloccare il cellulare in caso di perdita o furto	• Eff cel au
Fax in uscita (effettuabile solo da personale preventivamente autorizzato)	
• Controllare il numero di telefono chiamato • Aggiungere avvertenza sulla riservatezza sui documenti inoltrati • Verificare il corretto inoltro • Cancellare la memoria	• Dir • EFI INT

Maturity Model



INTERNATIONAL STANDARD

ISO/IEC 21827

Second edition
2008-10-15

Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)

Technologies de l'information — Techniques de sécurité — Ingénierie de sécurité système — Modèle de maturité de capacité (SSE-CMM®)

Reference number
ISO/IEC 21827:2008(E)

ISO IEC

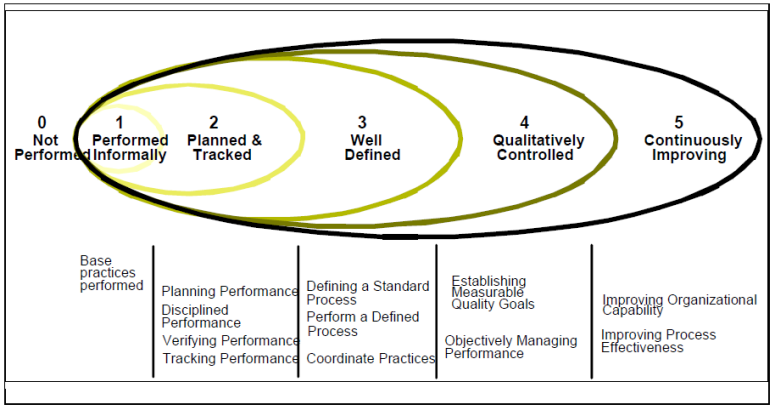
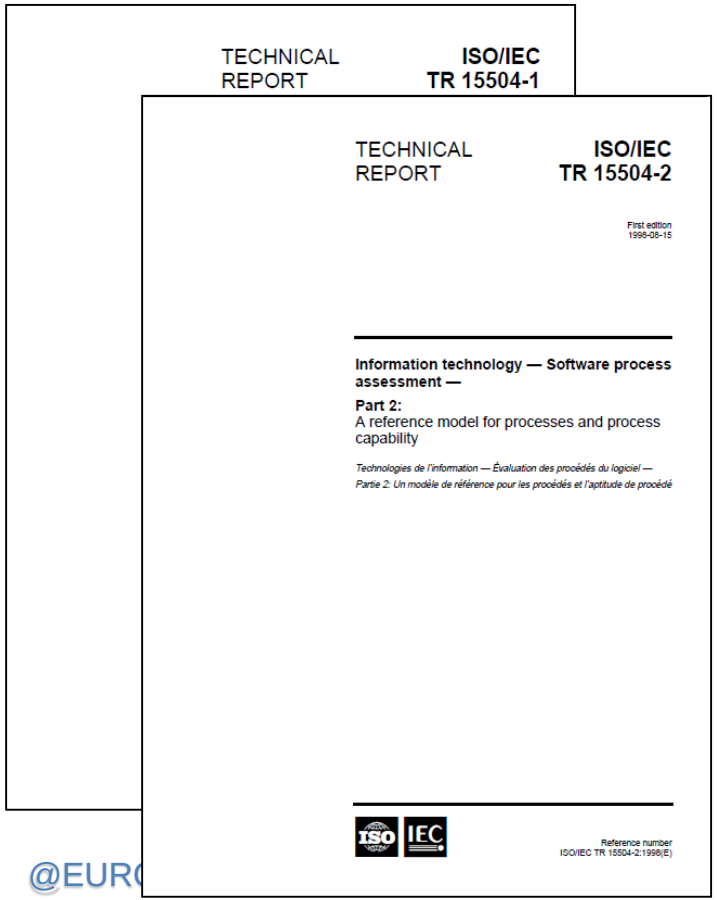


Figure 6 — Capability levels represent the maturity of security engineering organizations

Maturity Model



Level 0: *Incomplete.*

There is general failure to attain the purpose of the process. There are few or no easily identifiable work products or outputs of the process.

Level 1: *Performed.*

The purpose of the process is generally achieved. The achievement may not be rigorously planned and tracked. Individuals within the organization recognize that an action should be performed, and there is general agreement that this action is performed as and when required. There are identifiable work products for the process, and these testify to the achievement of the purpose.

Level 2: *Managed.*

The process delivers work products according to specified procedures and is planned and tracked. Work products conform to specified standards and requirements. The primary distinction from the Performed Level is that the performance of the process now delivers work products that fulfil expressed quality requirements within defined timescales and resource needs.

Level 3: *Established.*

The process is performed and managed using a defined process based upon good software engineering principles. Individual implementations of the process use approved, tailored versions of standard, documented processes to achieve the process outcomes. The resources necessary to establish the process definition are also in place. The primary distinction from the Managed Level is that the process of the Established Level is using a defined process that is capable of achieving its process outcomes.

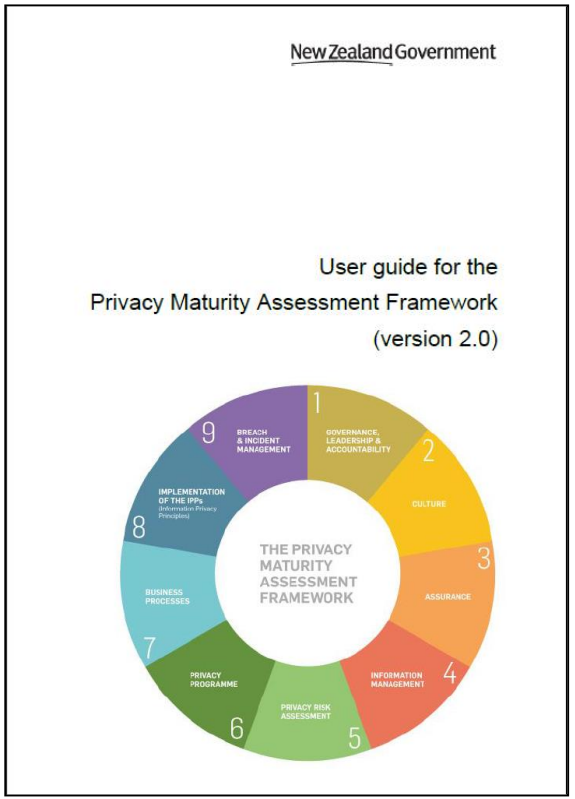
Level 4: *Predictable.*

The defined process is performed consistently in practice within defined control limits, to achieve its defined process goals. Detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict and manage performance. Performance is quantitatively managed. The quality of work products is quantitatively known. The primary distinction from the Established Level is that the defined process is now performed consistently within defined limits to achieve its process outcomes.

Level 5: *Optimizing.*

Performance of the process is optimized to meet current and future business needs, and the process achieves repeatability in meeting its defined business goals. Quantitative process effectiveness and efficiency goals (targets) for performance are established, based on the business goals of the organization. Continuous process monitoring against these goals is enabled by obtaining quantitative feedback and improvement is achieved by analysis of the results. Optimizing a process involves piloting innovative ideas and technologies and changing non-effective processes to meet defined goals or objectives. The primary distinction from the Predictable Level is that the defined and standard processes now dynamically change and adapt to effectively meet current and future business goals.

Privacy Maturity Model



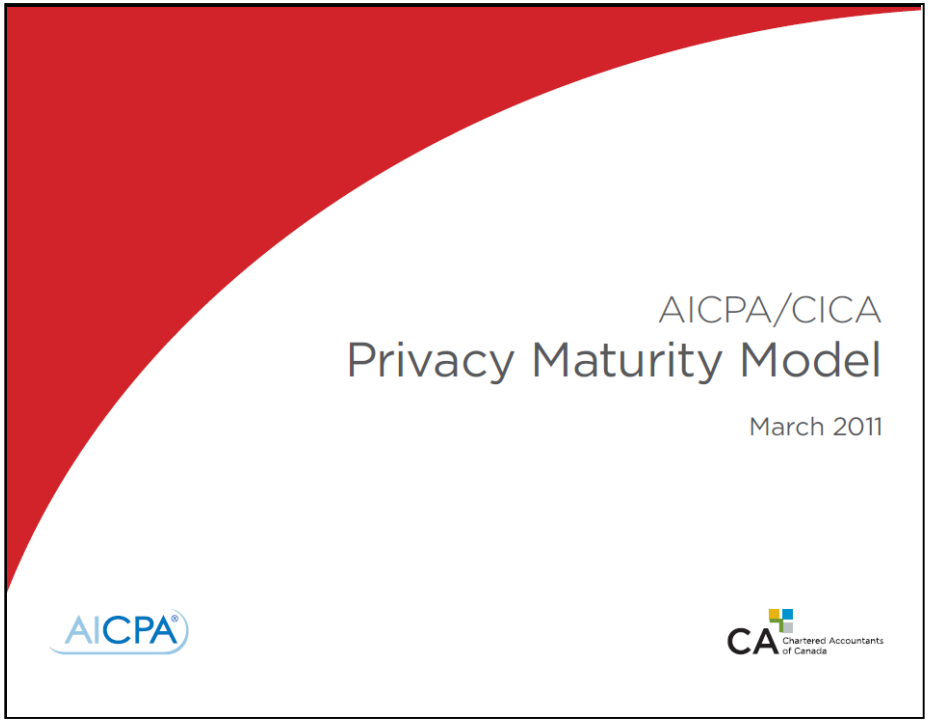
Maturity level	Description
N/A	Attributes are not applicable or a high priority, based on a mature understanding of organisational risks and risk appetites.
Ad hoc	Unstructured approach where privacy policies, processes, and practices are not sufficiently defined or documented. Privacy management is mostly dependent on initiatives by individuals rather than processes.
Developing	Privacy management is viewed as a compliance exercise and the overall approach is largely reactive with some documented guidelines. There is limited central oversight of the privacy policies, processes, and practices, with siloed approaches within business units.
Defined	Privacy policies, processes, and practices are defined and comprehensive to meet the operating needs of the agency and are consistently implemented throughout. The business has a holistic and proactive approach with widespread awareness of privacy management.
Embedded	Privacy management is embedded into the design and functionality of business processes and systems and is consistent across the agency. Well-defined governance and oversight structures exist.
Optimised	Privacy management is viewed as a strategic initiative with a clear agency culture of continuous improvement. The agency is viewed by stakeholders and the public as a leader in privacy management, introducing innovative initiatives to meet their needs.

Privacy Maturity Model

Privacy Maturity Assessment Framework: Elements, attributes, and criteria (version 1.0)

Ref	Element	Attribute	Maturity level ratings and criteria				
			Ad hoc	Developing	Defined	Embedded	Optimised
1	**Governance, leadership, and accountability**	**Senior leadership commitment**	Leadership commitment for comprehensive privacy management is not demonstrated. No support for or awareness of privacy initiatives. The privacy programme of work is not adequately resourced.	Leadership considers privacy as issues or breaches arise. Managers are aware of privacy initiatives within their business units. Management is aware of the resources and core skills needed to effectively deliver a privacy programme of work, but further resourcing is required.	Leadership is aware of the agency's privacy management and actively promotes it e.g. through information available on the agency's intranet, or regular agency-wide communications. Dedicated resources are allocated to deliver the privacy programme of work.	Leadership takes a proactive and integrated approach to leading privacy management. Resourcing for privacy is considered at a strategic level within the agency.	Leadership works collectively to seek innovative ways to continuously improve privacy management. Resources are deployed strategically to support the ongoing integration of the privacy framework into the business strategy. Information obtained through risk assessment or review of response to any identified breach is used to inform deployment of resources.
		Governance oversight	Limited or no reporting and access to the governance board /committee(s) / executive leadership team.	Established reporting lines to the governance board / committee(s), and access to the executive leadership team exist, but these are used largely in response to specific issues. Discussions on privacy are included in governance board / committee(s) / executive leadership team meetings, but these are largely in response to specific issues.	Governance board / committee(s) / executive leadership team receive regular updates on the privacy programme. Governance meetings include discussions on privacy issues and the effectiveness of the privacy programme.	Management proactively reports to the governance board / committee(s) / executive leadership team, to inform them of significant changes to the privacy risk profile. Governance meetings include discussions on the strategic direction of the privacy programme and privacy as an integral aspect of risk management.	Functional oversight of the privacy function and programme is included in the risk management organisational structure and is shown by setting policies and monitoring compliance. The governance board / committee(s) / executive leadership team actively informs business performance and improvements on privacy management.
		Management structure, roles, and responsibilities	Limited or no defined reporting structures for privacy management, issues, or improvement. No senior executive responsible for privacy management.	Some existing line management and reporting structures are in place for privacy management, issues, and improvement. A senior executive is formally responsible for privacy management, but has limited oversight or involvement in the privacy programme.	Formal and structured line management and governance over privacy management exists. There is formal responsibility and accountability for each element of the privacy programme and for the implementation of the Information Privacy Principles into the business. A senior executive is authorised to make decisions on privacy management, including the programme's content, approach, and resourcing. This person is accountable for privacy management and maintains oversight of the agency's privacy management.	Governance board / committee(s) / executive leadership team has a governance role in privacy (ie strategic decision-making and approval of policy) rather than undertaking day-to-day management of the programme. Senior management views privacy assessment and management as integral to their role.	Ongoing, regular, and formal discussions on privacy occur between the governance board / committee(s), and the executive management and senior management levels. A formal privacy management structure covering the entire agency is in place.

Privacy Maturity Model



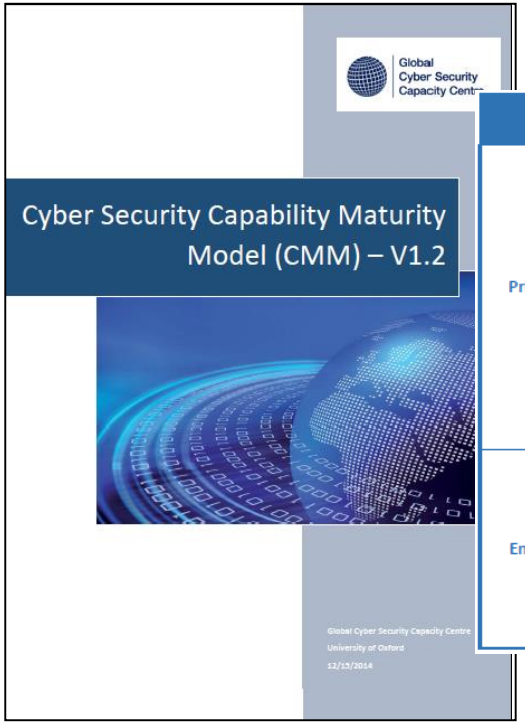
Ad hoc
Repeatable
Defined
Managed
Optimized

Privacy Maturity Model

AICPA/CICA PRIVACY MATURITY MODEL[1]
Based on Generally Accepted Privacy Principles (GAPP)[2]

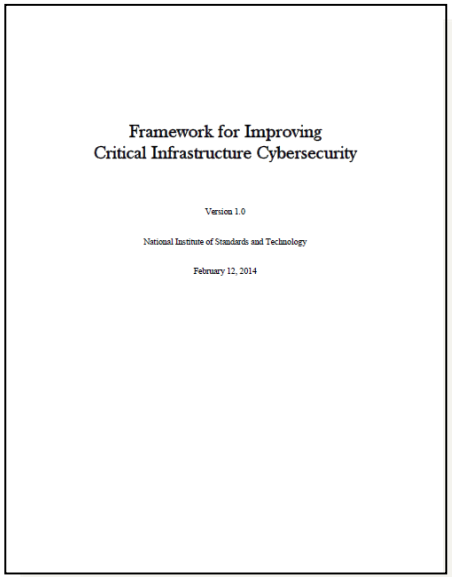
GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria)	**The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.**					
Privacy Policies (1.1.0)	**The entity defines and documents its privacy policies with respect to notice; choice and consent; collection; use, retention and disposal; access; disclosure to third parties; security for privacy; quality; and monitoring and enforcement.**	Some aspects of privacy policies exist informally.	Privacy policies exist but may not be complete, and are not fully documented.	Policies are defined for: notice, choice and consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring and enforcement.	Compliance with privacy policies is monitored and the results of such monitoring are used to reinforce key privacy messages.	Management monitors compliance with policies and procedures concerning personal information. Issues of non-compliance are identified and remedial action taken to ensure compliance in a timely fashion.
Communication to Internal Personnel (1.1.1)	**Privacy policies and the consequences of non-compliance with such policies are communicated, at least annually, to the entity's internal personnel responsible for collecting, using, retaining and disclosing personal information.** **Changes in privacy policies are communicated to such personnel shortly after the changes are approved.**	Employees may be informed about the entity's privacy policies; however, communications are inconsistent, sporadic and undocumented.	Employees are provided guidance on the entity's privacy policies and procedures through various means; however, formal policies, where they exist, are not complete.	The entity has a process in place to communicate privacy policies and procedures to employees through initial awareness and training sessions and an ongoing communications program.	Privacy policies and the consequences of non-compliance are communicated at least annually; understanding is monitored and assessed.	Changes and improvements to messaging and communications techniques are made in response to periodic assessments and feedback. Changes in privacy policies are communicated to personnel shortly after the changes are approved.

Security Maturity Model



D2-4: Privacy online					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Privacy Standards	Government discussions of privacy issues may have begun and include multiple stakeholders, but no privacy standards are in place.	Laws and policies promoting access to government and other public information are being considered.	All relevant actors from the private sector and civil society are actively driving change in practices, laws, and regulations that impinge on privacy. Government is considering adoption of human rights legislation with a focus on privacy.	Stakeholders comply with regionally and internationally recognised standards for human rights, particularly regarding privacy but implementation of these standards is not pervasive. Compliance with such standards provides strategic guidance for investment in privacy protection.	Domestic actors, policies and practices actively shape positive international perceptions of privacy and are central to informing multi-stakeholder decisions. Compliance to privacy components of the Universal Declaration of Human Rights is demonstrated, and research is conducted that considers the optimal application of human rights (and particularly privacy) to cyber security.
Employee Privacy	Minimal or no discussion among private sector leaders regarding privacy issues in the workplace exists.	Privacy in the workplace is recognised as an important component of cyber security and is beginning to be institutionalised in employee programs.	Employers maintain privacy policies that provide a minimum level of privacy for employees.	Employees are sensitised to their privacy rights within the organisation and individual privacy obligations are understood based on strategic planning. Compliance to human rights relevant best practices on privacy in the workplace is achieved.	Privacy impact assessments are regularly conducted and feed into policy revision.

Framework



Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

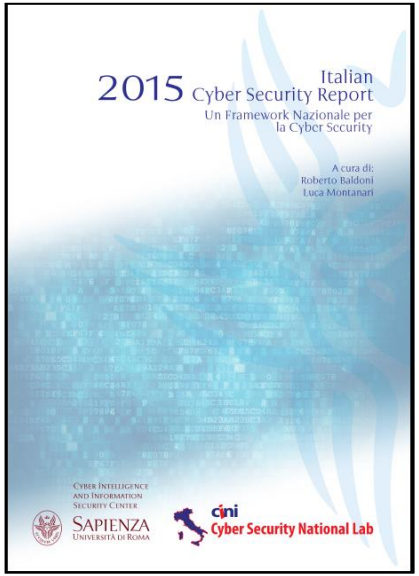
National Institute of Standards and Technology

February 12, 2014

Table 1: Function and Category Unique Identifiers

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

Framework



Functions	Categories	Subcategories	Priority Levels	Maturity Levels M1	M2	M3	M4	Informative References	Guide Lines
IDENTIFY									
PROTECT									
DETECT									
RESPOND									
RECOVER									

Framework

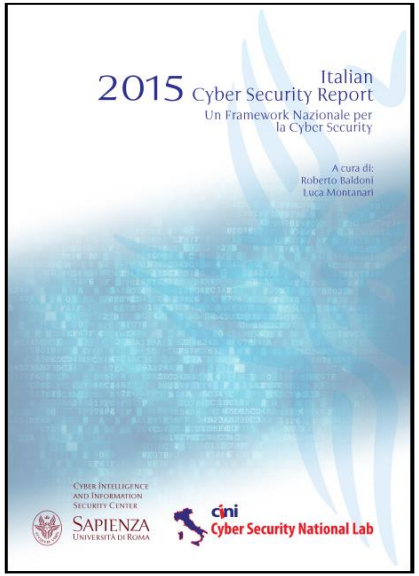


Tabella 3.1: Esempio di livelli di maturità per Subcategory "PR.AC-1: PR.AC-1:Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrate".

Livello	Descrizione
M1	Le identità e le credenziali sono amministrate localmente su ciascun dispositivo o sistema IT.
M2	Le identità e le credenziali sono amministrate attraverso una directory aziendale che consente l'applicazione omogenea di regole e livelli minimi di sicurezza.
M3	Specifiche soluzioni tecnologiche sono adottate per gestire in maniera specifica e appropriata le utenze privilegiate (es. Amministratori di Sistema).

Tabella 3.2: Esempio di livelli di maturità per la Subcategory "ID.BE-3: Sono definite e rese note delle priorità per quanto riguarda la missione, gli obiettivi e le attività dell'organizzazione".

Livello	Descrizione
M1	M1.1. L'azienda ha definito una strategia per la cyber Security.
M2	M2.1. All'interno della strategia sono definiti gli obiettivi e le attività di cyber Security dell'organizzazione. M2.2. La strategia è allineata con gli obiettivi strategici e rischi aziendali. M2.3. La strategia definisce l'approccio per la Governance della cyber security. M2.3. La strategia definisce la struttura e l'organizzazione per la realizzazione del programma. M2.4. La strategia è approvata dal Consiglio di Amministrazione.
M3	M3.1. La strategia è aggiornata regolarmente per tenere conto dei cambiamenti di business, cambiamenti nel contesto operativo, e cambiamenti nel profilo di rischio.

Key indicator: Lag indicators

- Misurano un risultato
- Sono facili da individuare
- Sono precisi
- Difficilmente confutabili
- Indicano la situazione attuale
- Non aiutano ad individuare le azioni da intraprendere

Key indicator: Lead indicators

- Misurano un processo per raggiungere un risultato
- Sono difficili da individuare
- Non danno garanzie di successo
- Sono più facilmente confutabili

Esempio

Sono in sovrappeso e desidero dimagrire

Lag indicator

peso rilevato sulla bilancia ogni mattina

Lead indicators

numero di calorie assunte

numero di chilometri di corsa effettuati

ore di palestra effettuate

Come definire dei lead Indicators

I testi di Governance dicono che per definire un insieme di *Lead indicators* è necessario :

- Scomporre il Processo che porta al risultato in una serie di attività
- Individuare «Buone pratiche» che definiscano come svolgere le attività
- Verificarne (misurarne) l'applicazione

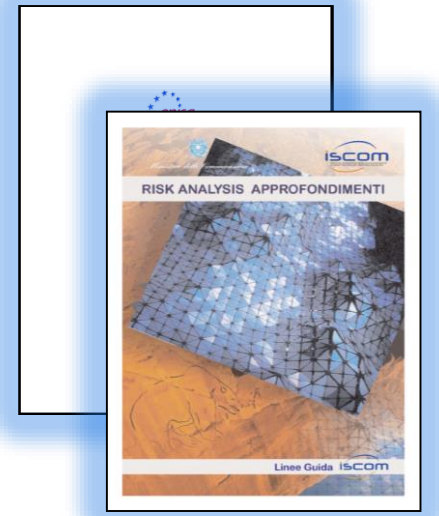
Key Performance Security Indicators

Name	Inventory of software or devices		
KPSI Index	1		
CAG Critical Control(s)	1, 2		
Description/rationale	This KPSI reflects the concept that asset inventory is at the basis of every ISMS. 70 % of all incidents are not registered or not managed devices.		
Core ISI 001 [1] mapping	IWH_UNA.1, VTC_NRG.1		
Additional ISI 001 [1] mapping	IWH_VNP.1 to 3, IWH_VCN.1, IWH_UNA.1, VTC_WFI.1, VTC_NRG.1		
State of the Art figure	2		
Level 0	**Level 1**	**Level 2**	**Level 3**
No policy, no process, no tools	Processes characterized for the organization but often reactive (reset after incidents). No tools	Processes systematically implemented. Tools usage	Processes continuously checked with the level of application and effectiveness evaluated (indicators, with well-defined periodic reporting processes toward upper levels)

Information Security Indicators

IEX_PHI.1: Phishing targeting company's customers' workstations spoiling company's image or business
Phishing involves a growing number of business sectors (financial organizations, e-commerce sites, online games, social sites etc.). It includes attacks via e-mail with messages that contain either malicious URL links (to forged websites) or malicious URL links (to malware laden genuine websites).
Base events
Customer reporting of a phishing attempt. **Frequency:** High frequency and strong impact on the image **Severity:** 2 **Detection means:** Manual production (via periodic tests of customers or users) **Detection level:** 2 (detection rate can be up to 80 %)
Indicator production
Base measure: Date of the event **Derived measure 1:** Number of events detected during the last 30 days **Derived measure 2:** Number of unique campaigns detected during the last 30 days. A unique campaign consists of a series of coordinated phishing attacks coming from a single origin within a given time slot, with an average of 6 attacks per campaign. **Indicator value:** Ratio of Derived Measure 2 to the media exposure (communication measurement specific to each professional sector) **State-of-the-art value:** (Derived measure 2) 20 campaigns per month in English language (relatively high scattering between companies in a given business sector, primarily depending on the media exposure)
Link with ISO/IEC 27002 [2]
No
Maturity KPSI
Will be available in the next version of the present document.

Analisi dei rischi quali/quantitativa



- *Austrian IT Security Handbook*
- *Cramm*
- *Dutch A&K analysis*
- *Ebios*
- *ISF methods*
- *ISO/IEC IS 13335-2*
- *(ISO/IEC IS 27005)*
- *ISO/IEC IS 17799*
- *ISO/IEC IS 27001*
- *ISO 31010*
- *IT-Grundschutz*
- *Marion (replaced by Mehari)*
- *Mehari*
- *Octave*
- *SP800-30 (NIST)*

- *AS/NZS 4360:2004 RISK MANAGEMENT*
- *BSA – Baseline Security Assessment*
- *Ce.TRA - Continuous e.Business Threat and Risk Analysis*
- *CRAMM*
- *Defender Manager*
- *EBIOS*
- *ERAM - Enterprise Risk Assessment and Management*
- *FIRM (Fundamental Information Risk Management)*
- *ISA – Information Security Assessment*
- *ISO/IEC 21827 - System Security Engineering, Capability Maturity Model*
- *NET.RISK*
- *NORA - Network Oriented Risk Analysis methodology*
- *OCTAVE® - Operationally Critical Threat, Asset, and Vulnerability EvaluationSM*
- *OSSTMM – Open Source Security Testing Methodology Manual*
- *PRA – Psychological Risk Assessment*
- *RAF - Risk Analyis Facility*
- *RISKWATCH (versione per l'Italia)*
- *SARA - Simple to Apply Risk Analysis*
- *SPRINT – Simplified Process for Risk Identification*
- *SSM - Scalable Security Model*

Analisi dei rischi qualitativa (ISCOM)

Vantaggi
• Sufficientemente semplici, intuitivi, veloci, poco costosi e non richiedono la disponibilità di dati precisi.
Svantaggi
• La valorizzazione data ai vari parametri è molto soggettiva e legata alla esperienza di chi effettua la valutazione ed alla conoscenza dei sistemi ed ambiente da analizzare.

Analisi dei rischi quantitativa (ISCOM)

Vantaggi
• Considerano un valore numerico, riconducibile molto spesso a un valore monetario che identifica la perdita conseguente al verificarsi di un evento dannoso. • Pur essendo metodi complessi è evidente che una corretta valutazione dell'opportunità o meno di adottare una certa contromisura può derivare solo dall'uso di tali metodologie.
Svantaggi
• Sono quindi molto difficili e possono differenziare di molto i risultati ottenuti a seconda che la perdita che viene considerata nel calcolo prenda in considerazione ad esempio il solo valore dell'asset coinvolto o anche le conseguenze sul business della perdita o indisponibilità dello stesso. • L'applicazione di un metodo quantitativo presuppone l'esistenza di una serie di dati di partenza.

Analisi dei rischi semi quantitativa (ISCOM)

Vantaggi
Svantaggi
• La possibilità di utilizzare algoritmi anche sofisticati non può aumentare il livello di qualità nella valutazione del rischio se la stima dei singoli parametri è errata; anzi, più il metodo è complesso e maggiore è il rischio che venga recepito come corretto, dimenticando la soggettività del dato iniziale.

Analisi dei rischi qualitativa

RISCHIO = IMPATTO X PROBABILITA’

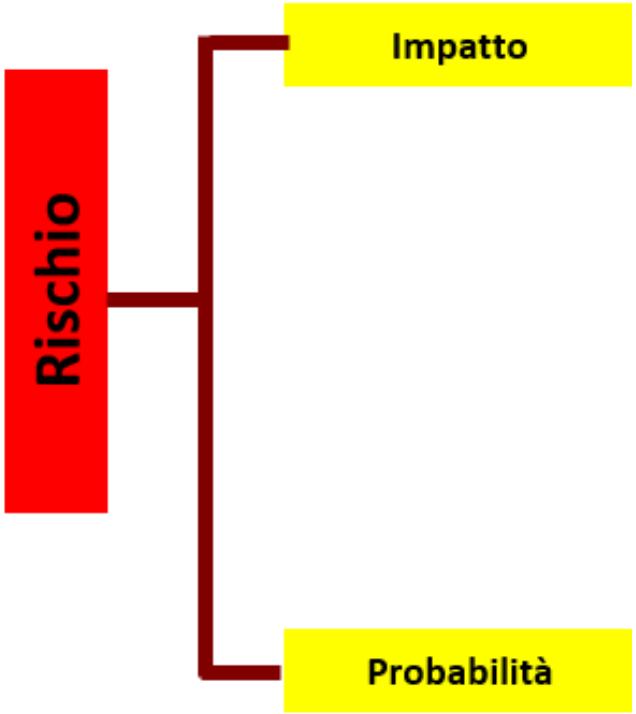
Analisi dei rischi quantitativa

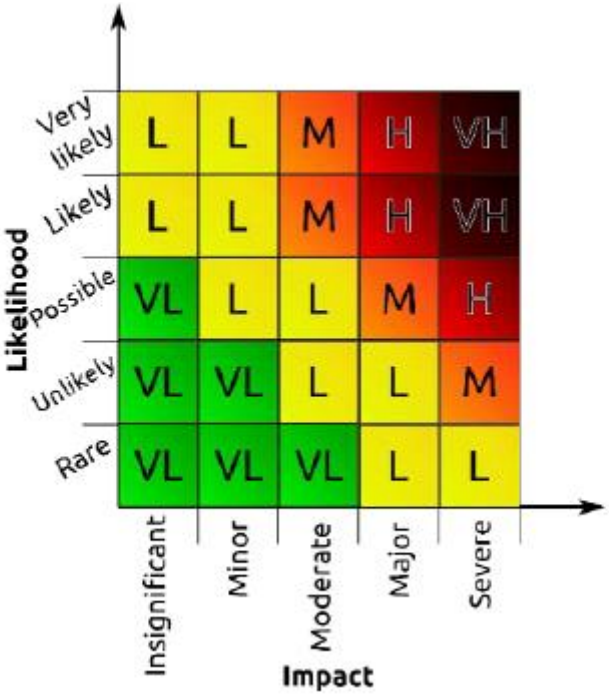
ALE = (Probability of event) x (value of loss)

$$ALE = \sum_{i=1}^{n} I(O_i)F_i$$

$\{O_1, O_2, \ldots, O_n\}$ – set of negative effects of event;
$I(O_i)$ – value expressed loss resulting from event,
F_i – frequency of i event.

Costruire un S.E. per l'analisi dei rischi

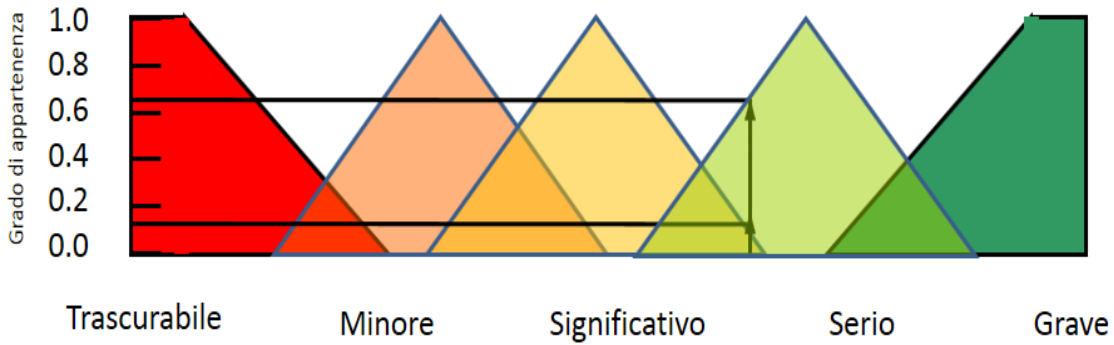




RISCHI	
VL	1
L	2
M	3
H	4
VH	5

Utilizziamo per l'esempio una matrice dei rischi basata su 5 valori di IMPATTO e 5 valori di PROBABILITA'

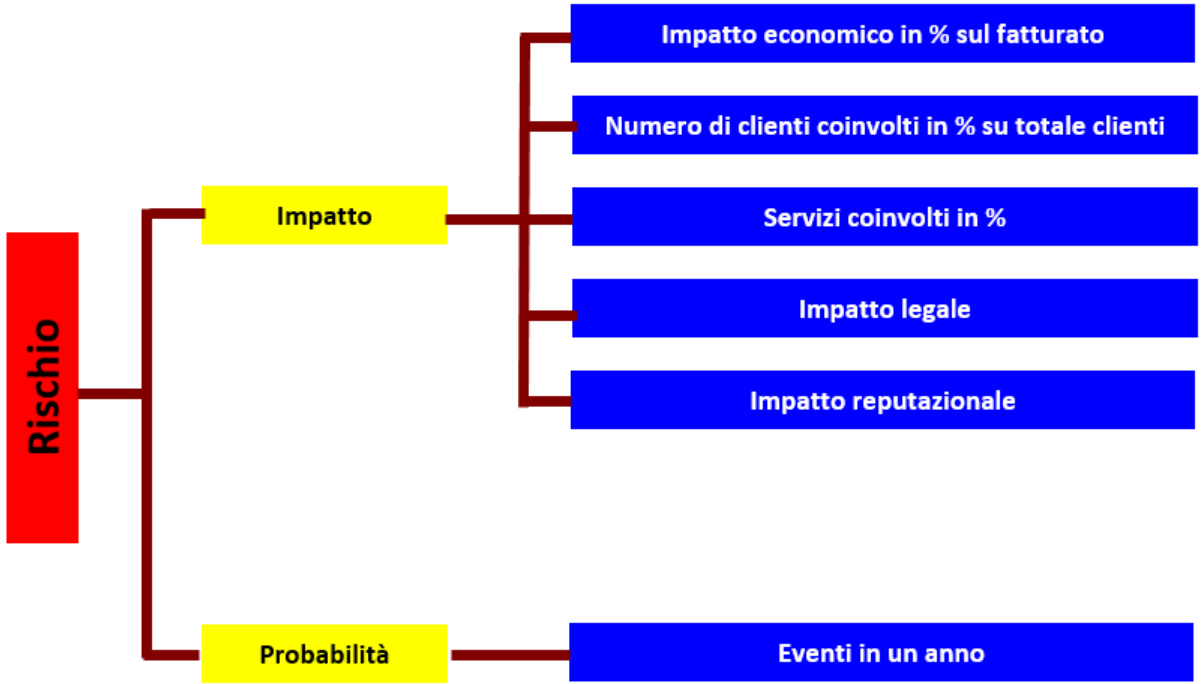
La logica fuzzy applicata all'analisi dei rischi



PROBABILTA'	
rare	1
unlikely	2
possible	3
likely	4
vwe likely	5

IMPATTO	
insignificant	1
minor	2
moderate	3
major	4
severe	5

Il modello


Rischio
Impatto
Probabilità
Impatto economico in % sul fatturato
Numero di clienti coinvolti in % su totale clienti
Servizi coinvolti in %
Impatto legale
Impatto reputazionale
Eventi in un anno

I valori elementari dell'impatto

IMPATTO LEGALE
Si
No

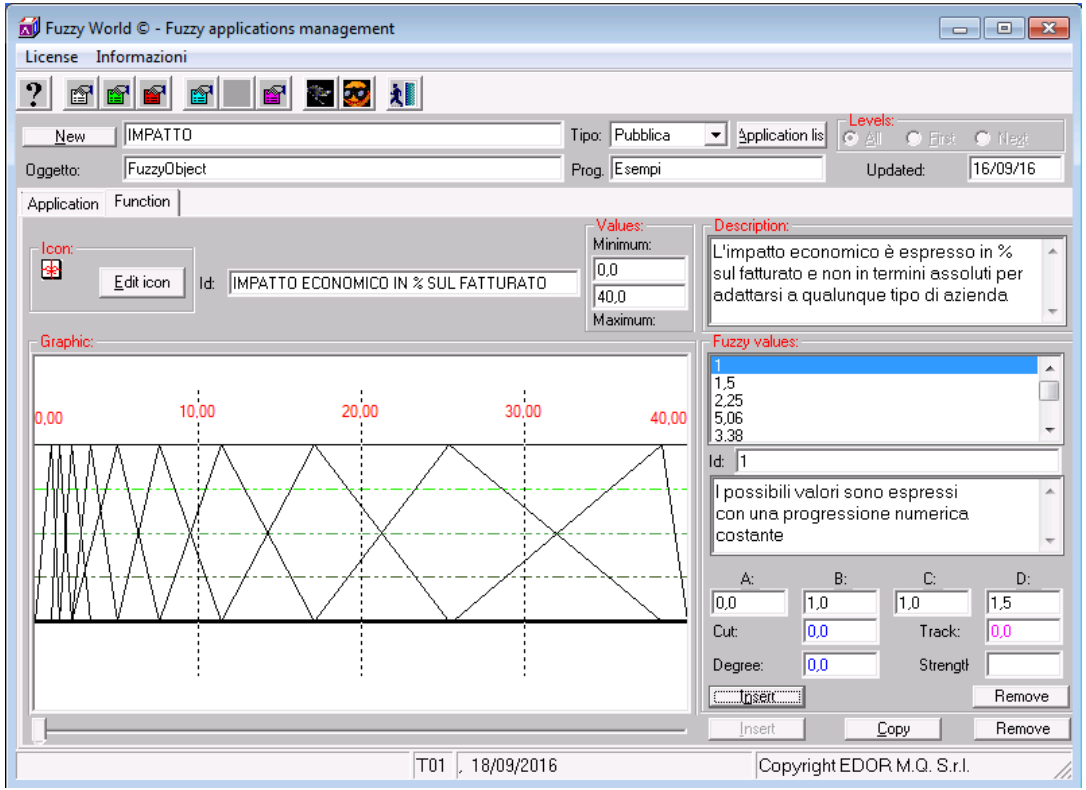
IMPATTO REPUTAZIONALE
Si
No

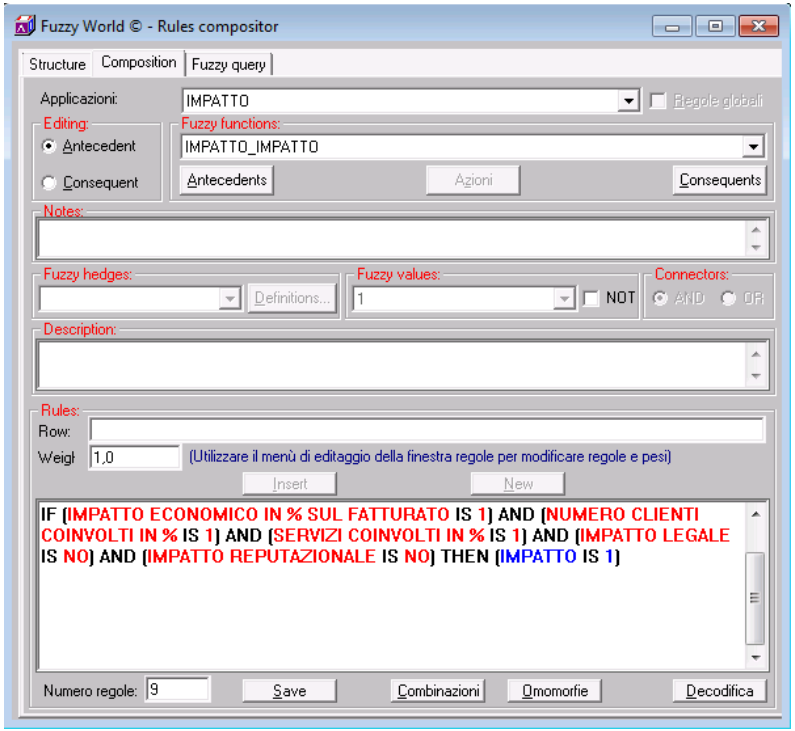
SERVIZI COINVOLTI IN %
1,00
1,50
2,25
3,38
5,06
7,59
11,39
17,09
25,63
38,44

IMPATTO ECONOMICO IN % SUL FATTURATO
1,00
1,50
2,25
3,38
5,06
7,59
11,39
17,09
25,63
38,44

NUMERO DI CLIENTI COINVOLTI IN % SU TOTALE CLIENTI
1,00
1,50
2,25
3,38
5,06
7,59
11,39
17,09
25,63
38,44

I valori elementari dell'impatto

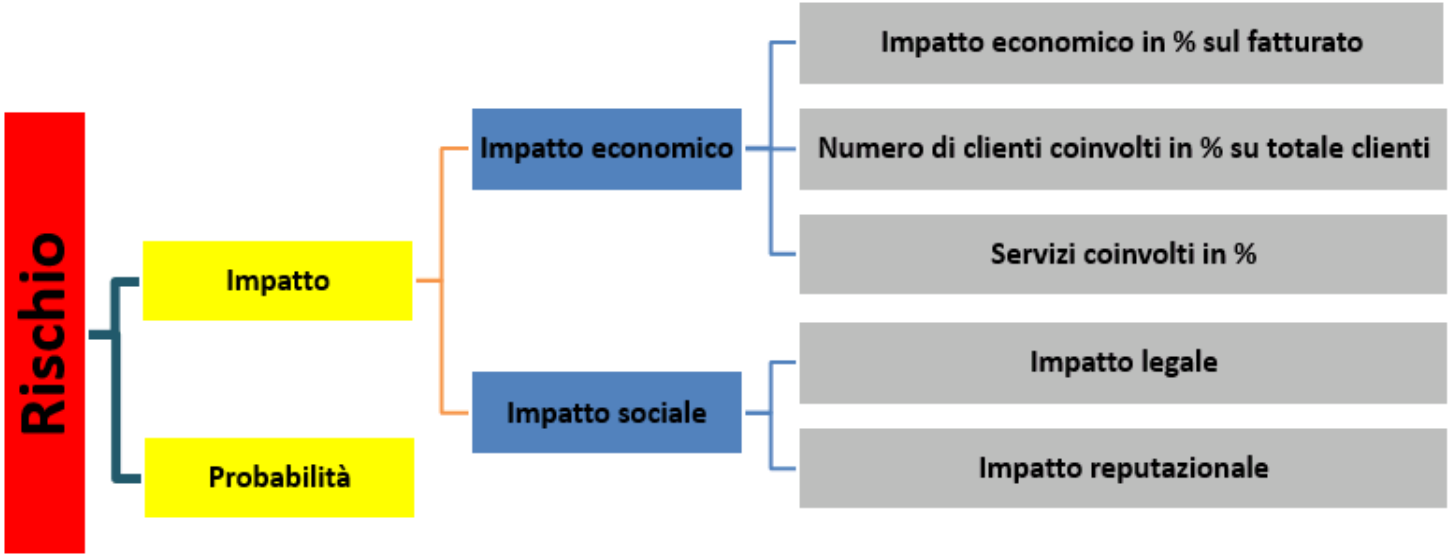




La soluzione basata su regole

Le 4000 regole vanno definite ed inserite manualmente.

Il modello

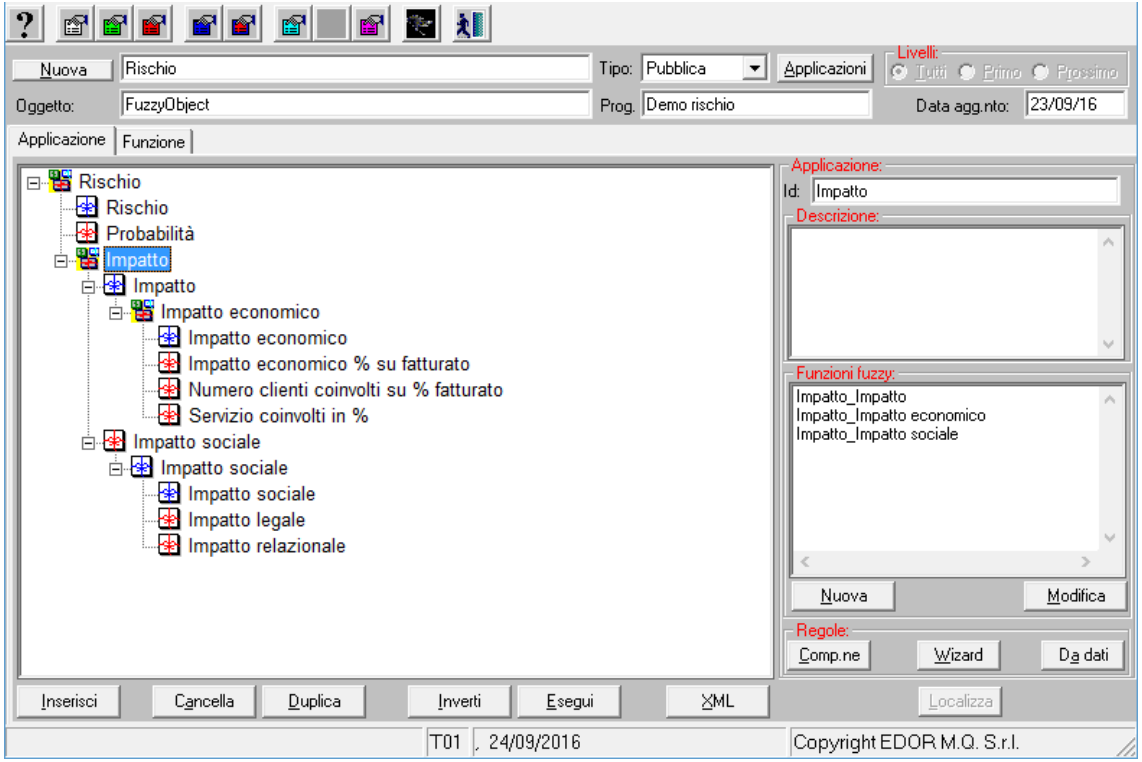

Rischio
Impatto
Probabilità
Impatto economico
Impatto sociale
Impatto economico in % sul fatturato
Numero di clienti coinvolti in % su totale clienti
Servizi coinvolti in %
Impatto legale
Impatto reputazionale

impatto economico in % sul fatturato	numero di clienti coinvolti in % su totale clienti	servizi coinvolti in %	Impatto economico	Pesi
1,00	0,00	0,00	1	1
1,50	0,00	0,00	1	1
2,25	0,00	0,00	1	1
3,38	0,00	0,00	1	1
5,06	0,00	0,00	1	1
7,59	0,00	0,00	2	1
11,39	0,00	0,00	2	1
17,09	0,00	0,00	2	1

Le soluzione basata su DI-RO

È possibile, in luogo che definire le singole regole, addestrare il sistema mediante l'importazione di dati esterni organizzati su fogli Excel

Il S.E. finale

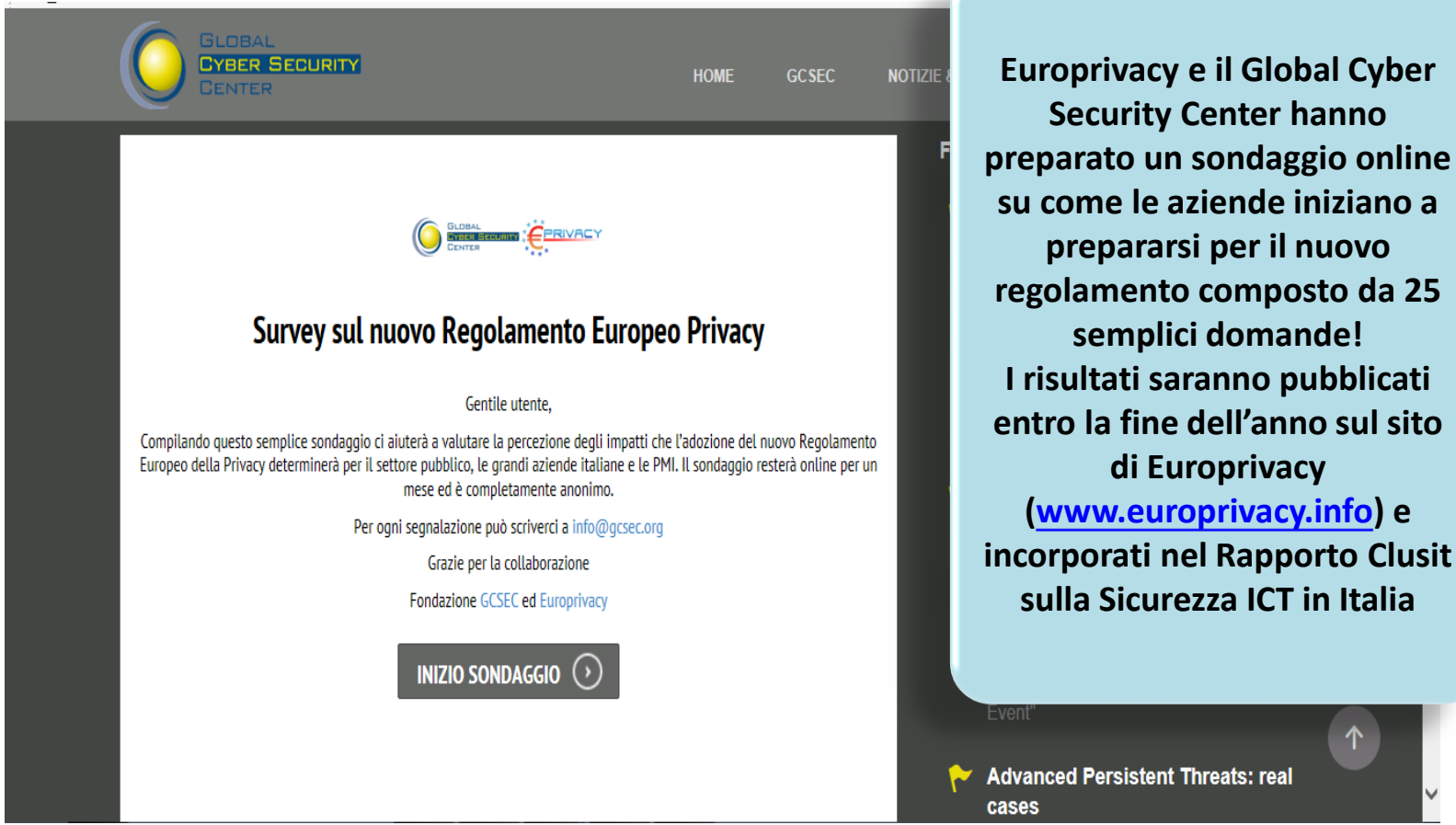

Nuova
Rischio
Tipo: Pubblica
Applicazioni
Livelli: Tutti Primo Prossimo
Oggetto: FuzzyObject
Prog. Demo rischio
Data agg.nto: 23/09/16
Applicazione
Funzione
Rischio
Rischio
Probabilità
Impatto
Impatto
Impatto economico
Impatto economico
Impatto economico % su fatturato
Numero clienti coinvolti su % fatturato
Servizio coinvolti in %
Impatto sociale
Impatto sociale
Impatto sociale
Impatto legale
Impatto relazionale
Applicazione:
Id: Impatto
Descrizione:
Funzioni fuzzy:
Impatto_Impatto
Impatto_Impatto economico
Impatto_Impatto sociale
Nuova
Modifica
Regole:
Comp.ne
Wizard
Da dati
Inserisci
Cancella
Duplica
Inverti
Esegui
XML
Localizza
T01 . 24/09/2016
Copyright EDOR M.Q. S.r.l.

Grazie per l'attenzione

Giancarlo Butti

giancarlo.butti@promo.it

cell. 338-9230742



Europrivacy e il Global Cyber Security Center hanno preparato un sondaggio online su come le aziende iniziano a prepararsi per il nuovo regolamento composto da 25 semplici domande!
I risultati saranno pubblicati entro la fine dell'anno sul sito di Europrivacy (www.europrivacy.info) e incorporati nel Rapporto Clusit sulla Sicurezza ICT in Italia