

L'iniziativa CISO Responsibilities Matrix (CisoRM)

CISO Cloud Summit

Alberto Manfredi
Presidente e Chapter Leader
MBA, CISSP, CISA, CRISC, CCSK, LA27001
alberto.manfredi@csaitaly.it

30 Novembre 2021

Comitato CISO Cloud

- Avviato il 30 Nov 2020 da CSA Italy.
- Il Comitato è un tavolo permanente di discussione e condivisione di informazioni ed esperienze che ha lo scopo di promuovere e perseguire gli obiettivi dell'associazione attraverso lo svolgimento delle seguenti attività:
 - ✓ Promuovere e valorizzare la figura del CISO attraverso diverse iniziative quali: profilazione del ruolo, definizione del percorso formativo (in particolare in ambito Cloud Security), analisi della sua collocazione nelle organizzazioni aziendali e relativo percorso di crescita, docenze in corsi/master e seminari.
 - ✓ approfondire temi inerenti alle ricerche in ambito Cloud Security effettuate da CSA (ad oggi sono attivi +35 gruppi di lavoro a livello internazionale con decine di pubblicazioni per anno),
 - ✓ condividere esperienze in ambito cloud security proposte dai singoli CISO,
 - ✓ partecipare a tavole rotonde, in presenza o virtuali, nell'ambito di eventi organizzati da CSA (in particolare in Italia ed EMEA),
 - ✓ effettuare peer-review su studi prodotti dai gruppi di lavoro CSA Italy.
- La missione ed attività del Comitato sono descritti nel Manifesto del Comitato CISO Cloud di CSA Italy <https://cloudsecurityalliance.it/ricerche/comitato-ciso-cloud/>

Il Comitato

Nicla DIOMEDE - *UNIVERSITA' DEGLI STUDI DI MILANO*

Alberto BORGONOVO - *SISAL*

Alessandro MARZI - *A2A*

Claudio FRENCIA – *STELLANTIS (FCA-PSA)*

Emanuele SCHIRRU - *SOSE*

Giampiero RASCHETTI - *BANCA POPOLARE DI SONDRIO*

Marcello FAUSTI - *ITALIAONLINE*

Marco TULLIANI - *ENGINEERING INGEGNERIA INFORMATICA*

Matteo BOLOGNINI - *NEXI*

Simone PEZZOLI - *AUTOSTRADe PER L'ITALIA*



Comunita' CISO Cloud

- Il Comitato è parte dell'iniziativa di sviluppo di una comunità, denominata **CISO Cloud Club**, aperta a tutti i professionisti che hanno un ruolo CISO o con responsabilità equivalenti, che decidono di contribuire alle attività promosse dal Comitato e dall'associazione CSA Italy.
- Ad oggi, più di **30** CISO italiani hanno aderito all'iniziativa promossa da CSA Italy.
- 2 Iniziative:
 1. *CISO Responsibilities Matrix (CisoRM)*
 2. *Valutazione dei Fornitori Cloud*



CISO Responsibilities Matrix

- La **CISO Responsibilities Matrix** è lo strumento a supporto della metodologia di auto valutazione delle responsabilità del ruolo di Chief Information Security Officer sviluppato dal Comitato CISO Cloud di CSA Italy. La CisoRM consente di correlare ogni responsabilità a specifiche attività, esperienze e formazione aiutando il CISO a:
 - ✓ monitorare nel tempo il livello qualitativo e quantitativo delle responsabilità assegnate, a supporto di eventuali richieste di adeguamento del livello organizzativo e/o contrattuale;
 - ✓ pianificare la formazione (specialistica e manageriale), indirizzandola sugli ambiti di responsabilità più critici;
 - ✓ presentare in modo complessivo le responsabilità del ruolo del CISO verso gli stakeholder, in particolare i livelli apicali dell'azienda, a supporto di una maggiore consapevolezza dell'importanza del ruolo in azienda.
- La CisoRM è disponibile gratuitamente a tutti i professionisti con ruolo CISO o equivalente e l'invio a CSA Italy (segreteria@csaitaly.it) della matrice CisoRM compilata consente di aderire alla comunità CISO Cloud dell'associazione (**CISO Cloud Club**)

CisoRM – La Matrice

6 Domini

32 Responsabilità

7 Criteri di Valutazione

CISO Responsibilities MATRIX (CisoRM)		SKILL LEVEL	DESIGN	OPERATE	VERIFY	APPROVE	TRAINING & EDUCATION			EXPERIENCE	NOTES
							Professional Courses/Certifications/Diploma	Bachelor/Laurea/MSc	Master/Post Laurea courses		
							Select from the top-down list in each cell	Select from the top-down list in each cell	Select from the top-down list in each cell		
SECURITY OPERATIONS	Security Monitoring										
	IT Project Management										
	IT Products and Services selection										
	Secure Information/Data Lifecycle										
	VA/PT										
	Asset Management										
	Patch Management										
	Configuration Management										
	Identity & Access Management										
	Threat intelligence										
	Reporting vs Constituency										
	Fraud & Reputation Management										
	Incident Management, Investigations and Forensics										
CIS (Communication and Information Systems)	CIS Governance & Operations										
GOVERNANCE & STRATEGY	DR&BC and Crisis Management										
	Security Architecture										
	Cloud & Digital Transformation Programs										
	Privacy Management										
	Security Policy Definition										
	Information Security Management										
	Information Security Risk Management										
	Third Party Risk Management										
	Reporting vs Board										
HUMAN RESOURCES	Security Training and Awareness vs Constituency										
	Team Management										
	Recruiting										
BUSINESS SUPPORT	Supply Chain										
	Partnership										
	Product / Service Life Cycle										
	Contracts										
BUDGET	Products and Services										
	Staff										

CisoRM – Domini e Responsabilita’

6 Domini

SECURITY OPERATIONS	Security Monitoring
	IT Project Management
	IT Products and Services selection
	Secure Information/Data Lifecycle
	VA/PT
	Asset Management
	Patch Management
	Configuration Management
	Identity & Access Management
	Threat intelligence
	Reporting vs Constituency
	Fraud & Reputation Management
	Incident Management, Investigations and Forensics
CIS (Communication and Information Systems)	CIS Governance & Operations
GOVERNANCE & STRATEGY	DR&BC and Crisis Management
	Security Architecture
	Cloud & Digital Transformation Programs
	Privacy Management
	Security Policy Definition
	Information Security Management
	Information Security Risk Management
	Third Party Risk Management
	Reporting vs Board
HUMAN RESOURCES	Security Training and Awareness vs Constituency
	Team Management
	Recruiting
BUSINESS SUPPORT	Supply Chain
	Partnership
	Product / Service Life Cycle
	Contracts
BUDGET	Products and Services
	Staff

32 Responsabilità

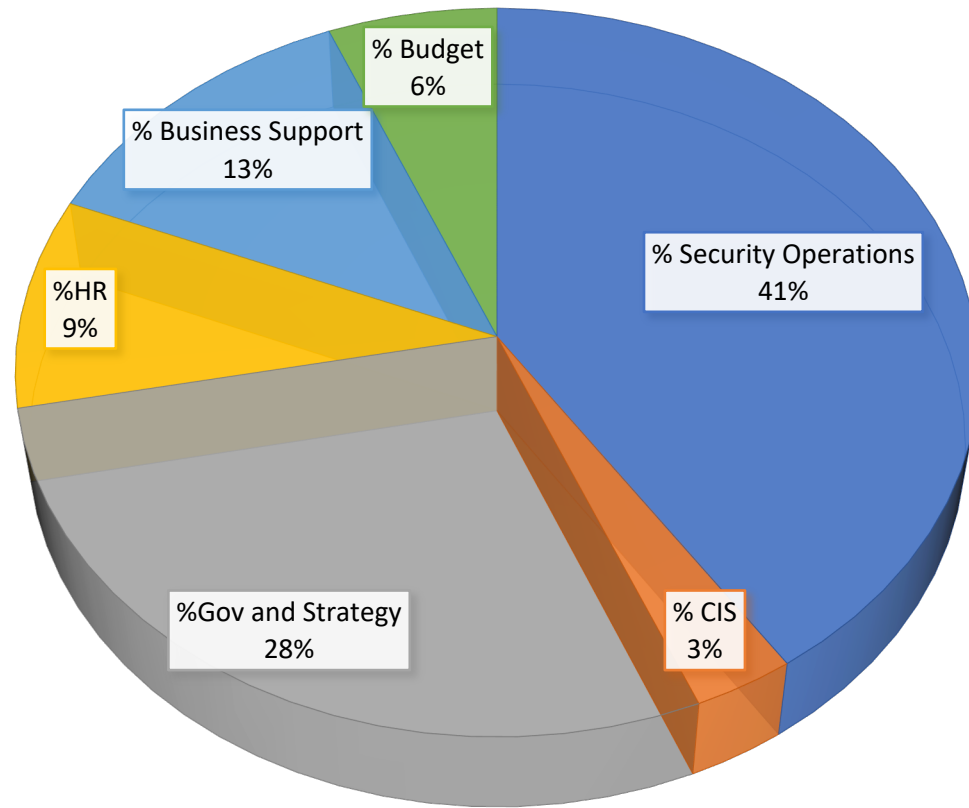
CisoRM – Criteri di Valutazione

SKILL LEVEL	DESIGN	OPERATE	VERIFY	APPROVE	TRAINING & EDUCATION			EXPERIENCE
					Professional Courses/Certifications /Diploma	Bachelor/Laurea/MSc	Master/Post Laurea courses	
1=Professional 2=Expert 3=Master	3=full responsibility 2=co-responsibility (i.e. with CIO/CSO), 1=contributor only	3=full responsibility 2=co-responsibility (i.e. with CIO/CSO), 1=contributor only	3=full responsibility 2=co-responsibility (i.e. with CIO/CSO), 1=contributor only	3=full responsibility 2=co-responsibility (i.e. with CIO/CSO), 1=contributor only	Select from the top-down list in each cell	Select from the top-down list in each cell	Select from the top-down list in each cell	# cumulative years. (Considering also experiences prior CISO role)

SCORE = (SKILL LEVEL) x (DESIGN+OPERATE+VERIFY+APPROVE) + (TRAINING & EDUCATION) + (EXPERIENCE)

PERSONAL SCORE	% Security Operations	% CIS	%Gov and Strategy	%HR	% Business Support	% Budget
0	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%

CisoRM – Impatto relativo per Dominio



Considerazioni finali



Grazie !



CSA Italy Website

<https://cloudsecurityalliance.it>



Community

<https://circle.cloudsecurityalliance.org>



LinkedIn

<https://www.linkedin.com/company/csa-italy>



Twitter

@CSA_Italy



Facebook

<https://www.facebook.com/CSAItaly>



Email

info@cloudsecurityalliance.it

