CSA | Italy Chapter

CISO
A job in search of a description

CISO Cloud Community
Working Group
“CISO Responsibilities Matrix”

Acknowledgments

Co-Chairs
Manuela Italia
Davide Del Vecchio
Alberto Manfredi

Contributors
Manuela Italia
Davide Del Vecchio
Matteo Colella
Alessandro Oteri
Alberto Manfredi

Reviewers
CISO Cloud Committee
CxO Trust Committee
CSA Italy Board

EXECUTIVE SUMMARY

The massive increase of cyber-attacks volume and complexity accelerated by various and recent global events and new pressures coming from authorities and regulations are pushing organizations to discover and establish a CISO role to build and oversee appropriate Information Security Management Systems. Italian organizations are aligned to this trend, also encouraged by the setup of the Italian National Agency for Cybersecurity (ACN) in 2021 that aims to protect the national cyberspace, to sustain the digital development of the country, and to promote public-private initiatives to strengthen the national cybersecurity and resilience posture.
In this context, **the growth and the evolution of the CISO role is being as fast as it is not clearly outlined**.

Just 20 years ago “cybersecurity” simply did not exist as a word.
It was referred to as “IT Security”, that later became “Information Security” and just a few years ago experts and newspapers started to use the term “cybersecurity”. In the same way, people responsible for cybersecurity in the early 2000 had an “IT Security manager” job title that later became “Information Security manager”, recently called “cybersecurity manager” and often including other buzzwords such as “resilience”.

While technology and cyber were growing and **started to be perceived as a business value** by companies, cybersecurity professionals were getting more and more important in the organizations. That is why, a few years ago, a C-level cyber position has begun to gain a foothold in the market.

However, differences in the core businesses, sizes and culture of companies lead to **a very fragmented situation** when trying to understand **where the CISO and its cybersecurity function sit in the organizations**.

- Am I asking for too much budget to execute the cyber strategy?
- Am I paid in line with the market?
- Am I asking too many people for my team?
- Should my role include more or less responsibilities?

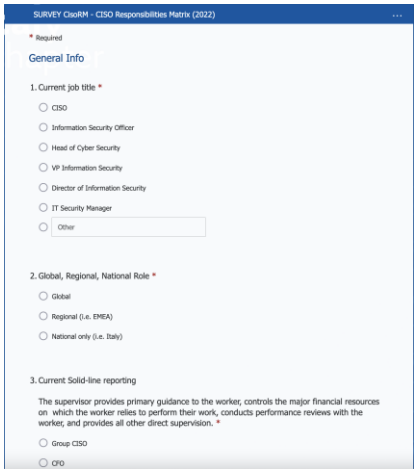
These are just a few of the questions that many CISOs and companies are trying to answer and that prompted the CISO Cloud Committee of CSA Italy to start the CISO Responsibilities Matrix (CISORM) project.

CISO RESPONSIBILITIES MATRIX (CISORM) PROJECT

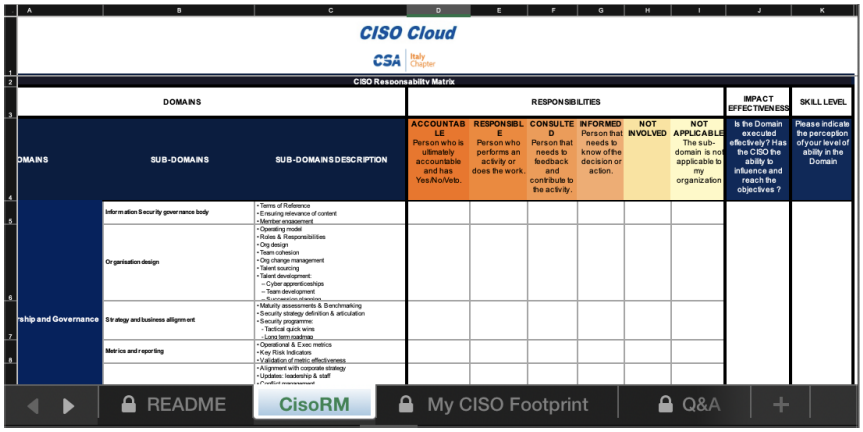
The CISO Cloud Committee is a community founded in 2020 and composed of over 40 Italian CISOs as a permanent roundtable to share information and experience among.
The CISORM project started framework one year ago with the aim to provide CISOs with **a tool to assess, represent and benchmark** her/his role.
The methodology considers the role context (industry, size, salary, etc..) and different relevant factors (responsibilities, skill levels and impact effectiveness) for each Information Security domain.

CISO Cloud Committee members have been invited to **complete the online survey** and anonymously share the following data:

- Role context information - Company Industry and Size, Salary, Contractual Grade, Years of experience, Team Size, Annual Budget, etc.
- RACI* Role responsibilities - for each Information Security domain (8) and sub-domain (45)
- Role Impact Effectiveness - a synthetic and qualitative personal judgment to represent with a score if the CISO is operating effectively with the ability to influence and reach his/her objectives
- Personal degree of expertise - according to the organization needs and expectations



All surveyed can download the **CISO Responsibility Matrix worksheet** to privately track and store the responses and make whatever analysis and reporting needed for her/his benefits.



Moreover, once filled, the worksheet automatically calculates "**My CISO Footprint**" that the CISO can use to **benchmark the positioning and variations of her/his role over time.**

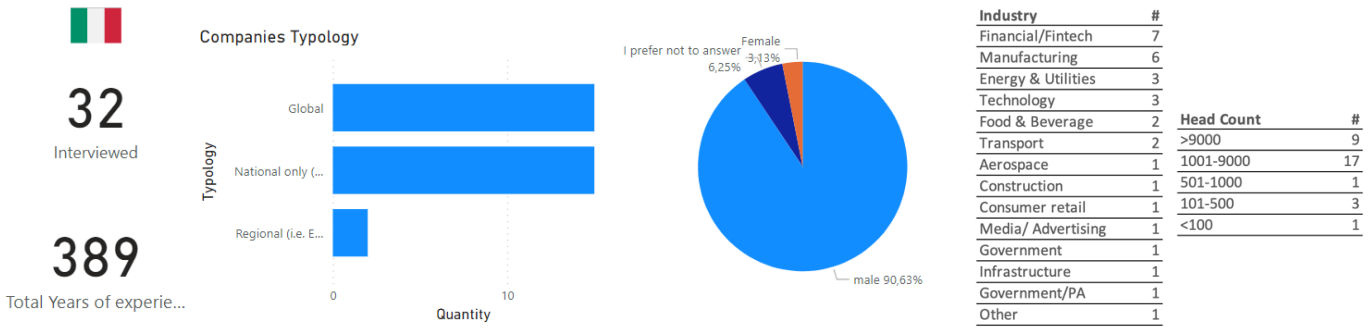
The CISO Responsibilities Matrix (CisoRM) **can help a CISO** to

Assess	Present	Enable discussions	Benchmark	Monitor & improve
Assess the role and identify actions to improve and plan initiatives on skills, processes, organization, governance and operating models for the various Information Security domains.	Present views on the current and evolving CISO role, increasing the awareness on the role importance to relevant organizations stakeholders.	Enable discussions on weaknesses and factors of concern, providing a level of detail and deep dive to enable decision making and to focus on significant matters at the organization level.	Benchmark of the positioning and variations over time and across organizations of the role, responsibilities, skills.	Monitor and improve her/his career development journey.

and **will help the CISOs community** to gain a better understanding of the role. Infact, the CISORM Workingroup anonymously collected the responses from a first CISOs sample through the Online Survey and started performing an initial data analysis and reporting.

INITIAL RESULTS & HIGHLIGHTS

SAMPLE CONFORMATION

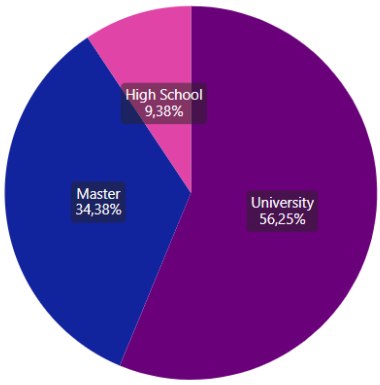


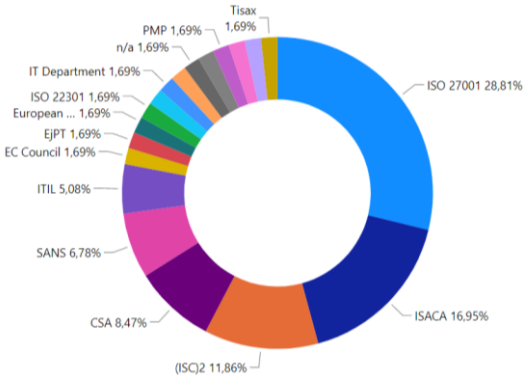
Industry	#
Financial/Fintech	7
Manufacturing	6
Energy & Utilities	3
Technology	3
Food & Beverage	2
Transport	2
Aerospace	1
Construction	1
Consumer retail	1
Media/ Advertising	1
Government	1
Infrastructure	1
Government/PA	1
Other	1

Head Count	#
>9000	9
1001-9000	17
501-1000	1
101-500	3
<100	1

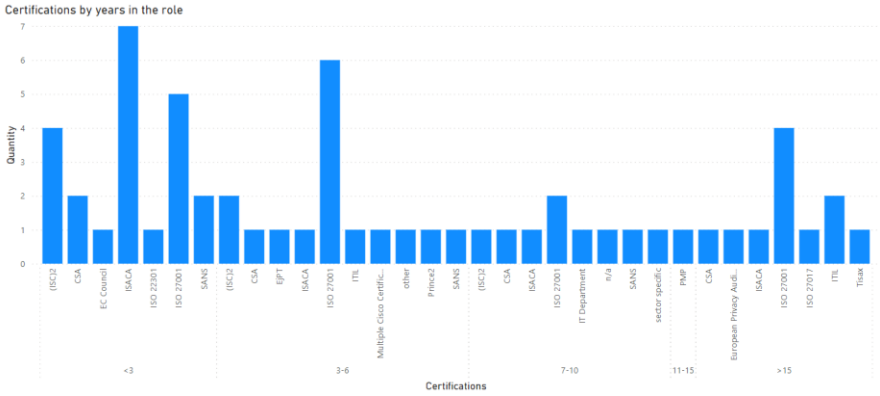
Due to the limited size of this first sample, at this stage this data should not be seen as a market reference benchmark. For the same reason, broad clusters and categories have been aggregated to provide summary averages and statistics.
CSA Italy cannot guarantee the accuracy and completeness of the information collected from surveyed or eliminate the possibility of anomalies, therefore CSA Italy accepts no liability whatsoever for any loss or damage caused by use of or reliance on this information.

EDUCATION





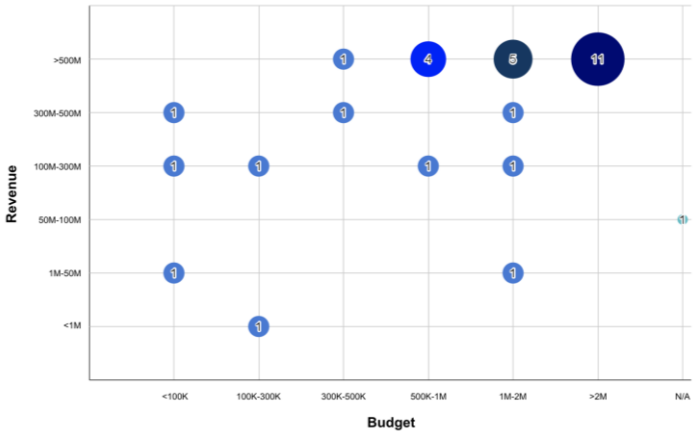
The distribution of certifications obtained shows an evident percentage in favor of ISO27001, followed by ISACA and (ISC)²

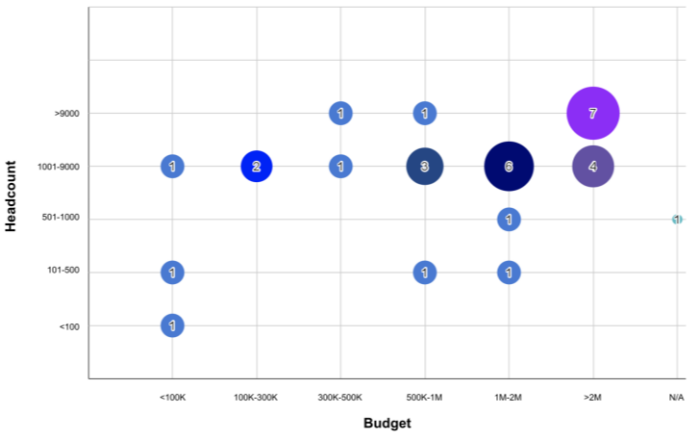


Certifications obtained by the CISOs sample vary according to the years spent in the role. ISACA, ISO and (ISC)2 certifications are common under three 3 years of experience.

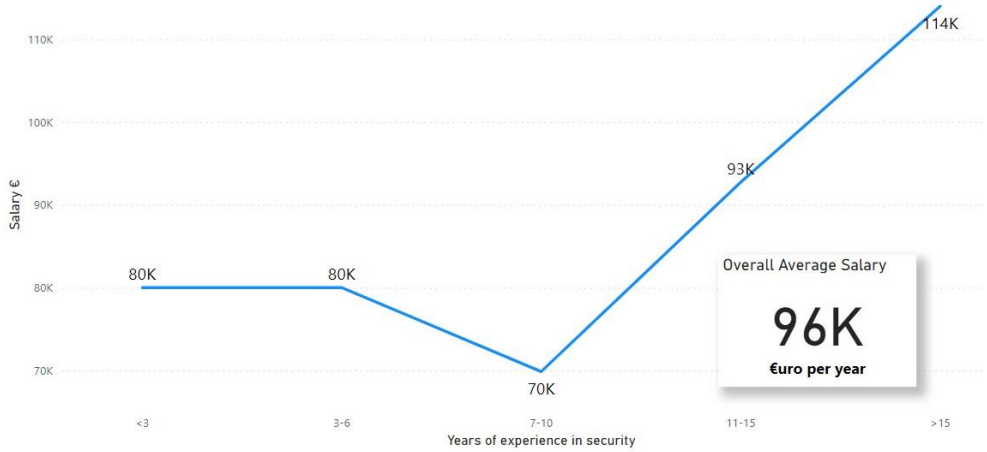
ECONOMICS

Budget allocated for cybersecurity shows a growing trend based on companies' size (Revenue and Headcount).

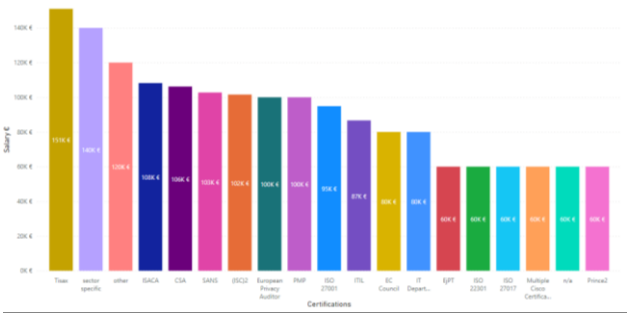




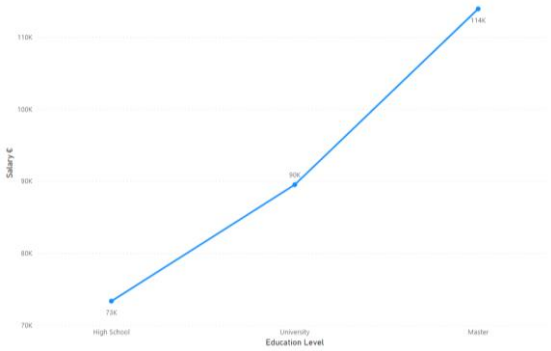
Average **CISOs salary** increases with years of experience in the security field.



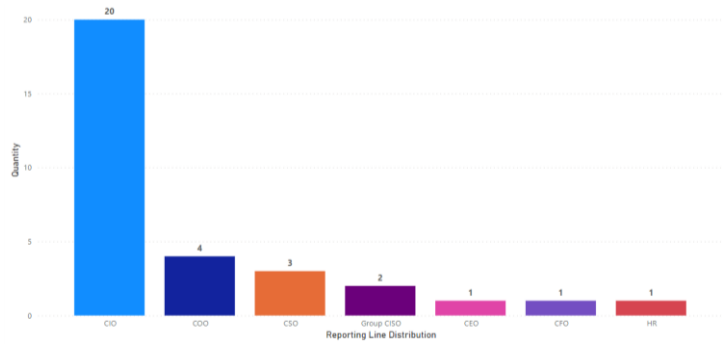
Average salary by obtained certification



An increase of the salary based on education level has been recorded: CISOs with a higher education receive a 60% higher salary



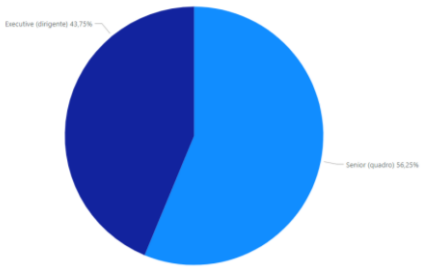
REPORTING LINE, JOB TITLE & CONTRACT



Most of the CISOs sample **reports to the CIO**, following at a great distance the COO and other functions.

Job Title	#
CISO	24
Head of Cyber Security	3
IT Security Manager	3
Head of IT Security	1
Operation Manager	1

75% of the sample has a CISO job title



More than half of the sample does not have an executive contract level.

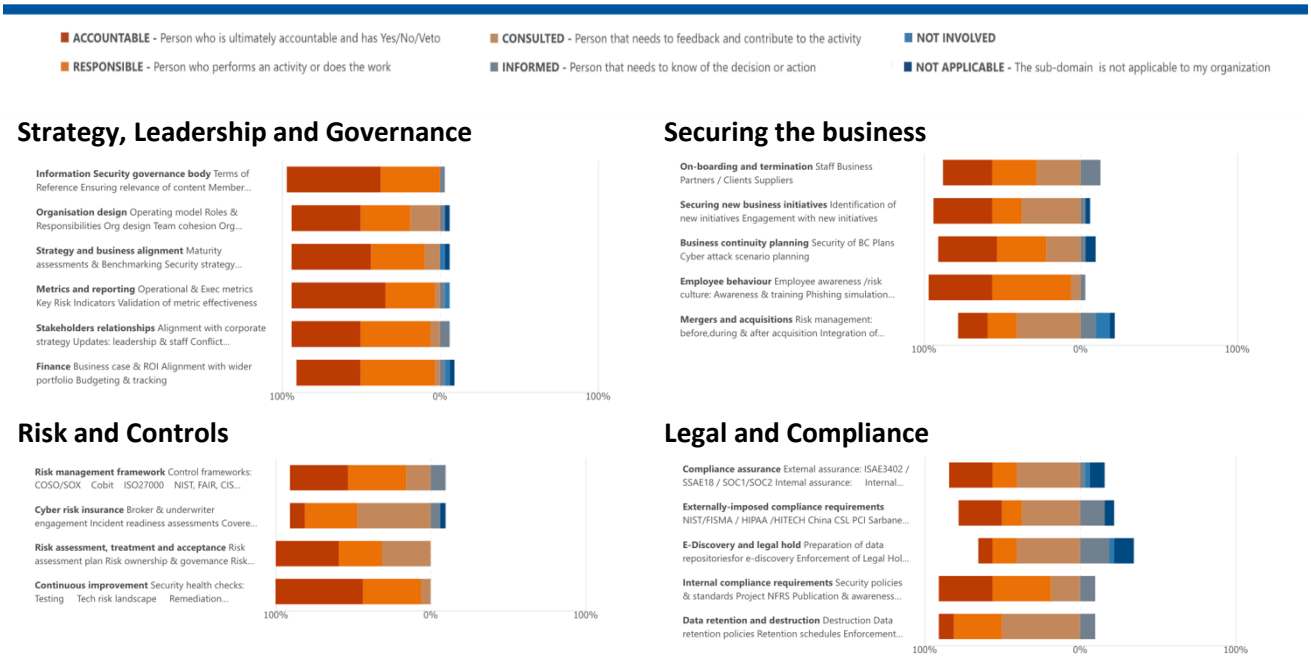
RESPONSIBILITIES

Almost all CISOs surveyed **is influencing** the 8 security domains, with **more focus on strategy and technology**.

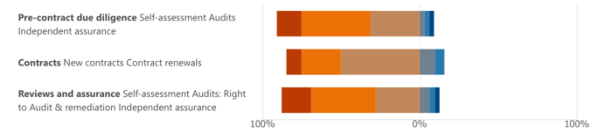
9.4% of the surveyed CISOs are **not involved in new applications design and in M&A** initiatives. The involvement of the CISO at the initial stages of new initiatives is crucial to identify, assess, and manage the potential risks that pose to the organization and its business.

Moreover, on a metric based on 5 points:

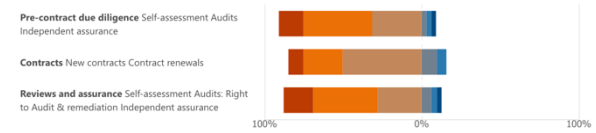
- CISOs feel **less effective** (rating around 3) on the "**Securing new initiatives**", "**Securing supply chain**" and "**Securing the business**" domains.
- CISOs feel to be **more effective** on "Security Operations" (3.73) and "**Strategy, Leadership and Governance**" (3.59) domains.



Securing supply chain

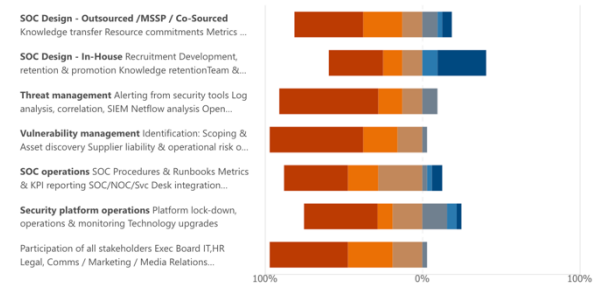


Securing new initiatives



Securing the Technology

Security Operation



WHAT'S NEXT

The CISO responsibility matrix (CISORM) is quite young and the roadmap for the next coming months is ambitious: becoming the barometer for the CISOs community around the topic of "what does it mean to be a CISO today".
The framework allows users to share a common approach to the role, based on the different data and benchmarks available, helping also the CISO to monitor and track the self-evaluation regarding her/his career development plan, in terms of responsibilities and skills through the footprint tool.

Some hints for the next steps of the methodology:

- Encourage other CISOs to participate to the CISORM initiatives to increase the sample and gain elements from different companies and sectors
- Promote the usage of CISORM as a periodic self-assessment for CISOs, to track the own progresses and changes in their role and context.
- Continue to improve the methodology also considering this first analysis exercise and feedback received by surveyed CISOs through the "feedback submission" function.

Permanent and official location for this report: https://www.cloudsecurityalliance.it

CSA Italy - Via Cesare Beruto 11 20131 Milano - C.F. 97673120586 - www.cloudsecurityalliance.it