# Collaborazione fattiva CIO-CISO: elemento base per una reale ed efficace sicurezza digitale

Marco R. A. Bozzetti, Presidente AIPSI

Pasquale De Martino, Vice Presidente CIO Club Italia


## Webinar AIPSI – CIO Club Italia
## 18 ottobre 2022

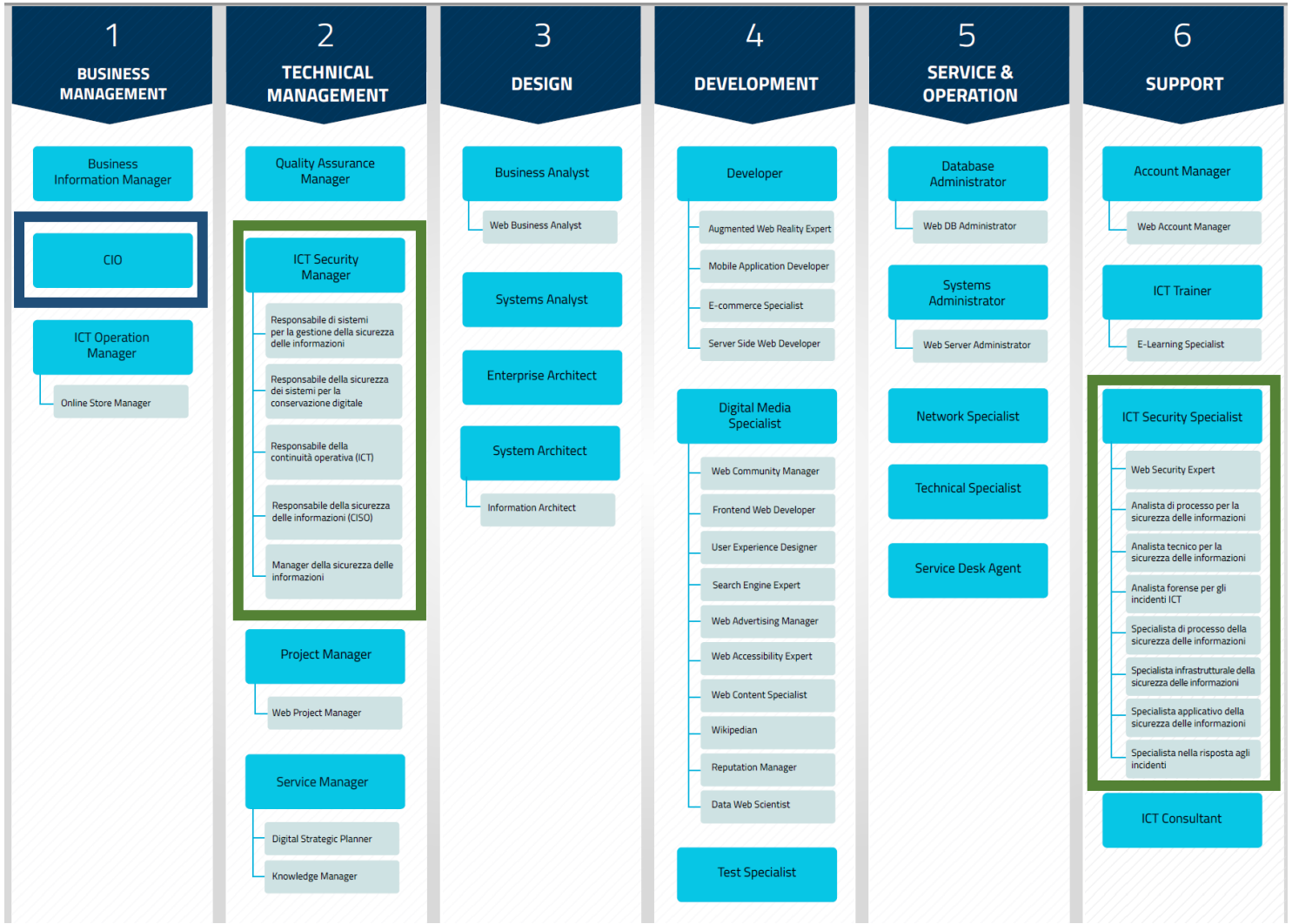
aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

CIO club

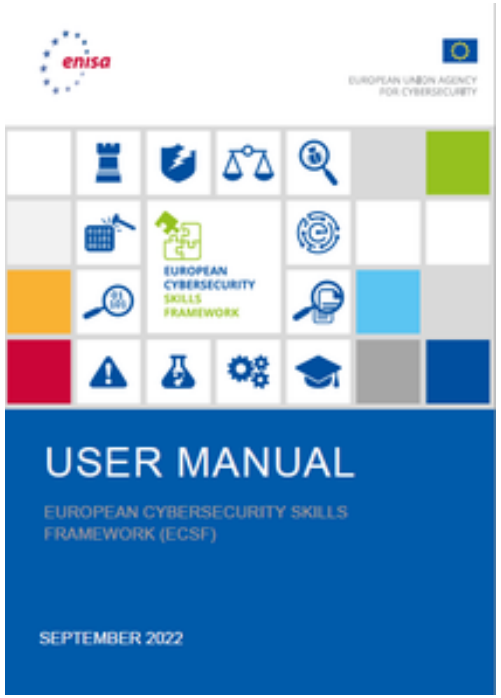
# Il ruolo del Sistema Informativo (SI) per il business nell'attuale società (ed economia) dell'informazione


- Ogni attività si basa ormai su applicazioni del Sistema Informativo
- Il Sistema Informativo non può che operare su Internet, ed è quindi esposto ad attacchi dall'esterno, oltre che dall'interno
- Il corretto, continuo e sicuro funzionamento del Sistema Informativo deve/dovrebbe garantire:
  - la **continuità operativa** (business continuity)
  - **l'integrità dei dati**
  - il mantenimento del vantaggio competitivo rispetto ai competitori
  - la compliance alle varie normative: GDPR per la privacy, L. 231, etc.
- Le informazioni del Sistema Informatico sono un **bene (asset) aziendale**, e come tali vanno protette e gestite
- **La sicurezza digitale** non è solo un problema tecnico, ma **di business**, dato che deve garantire la continuità operativa → **deve pertanto vedere coinvolto il vertice aziendale**

# Classificazione competenze AgID (derivata da eCF - EN 16234 1:2016)



# ENISA ECSF, European Cybersecurity Skills Framework (fa riferimento alle competenze eCF)


# L’opportunità di terziarizzare, soprattutto per le piccole realtà

## MSS

## Managed Security Services

**Terziarizzazione della gestione operativa della sicurezza digitale**:

- erogata da uno o più consulenti, o da una o più aziende specializzate
- totale o parziale (soluzione ibrida)
- svolta con strumenti informatici inseriti all’interno del Sistema Informativo stesso, o esterni, di proprietà dei e/o utilizzati dalle terze parti coinvolte.

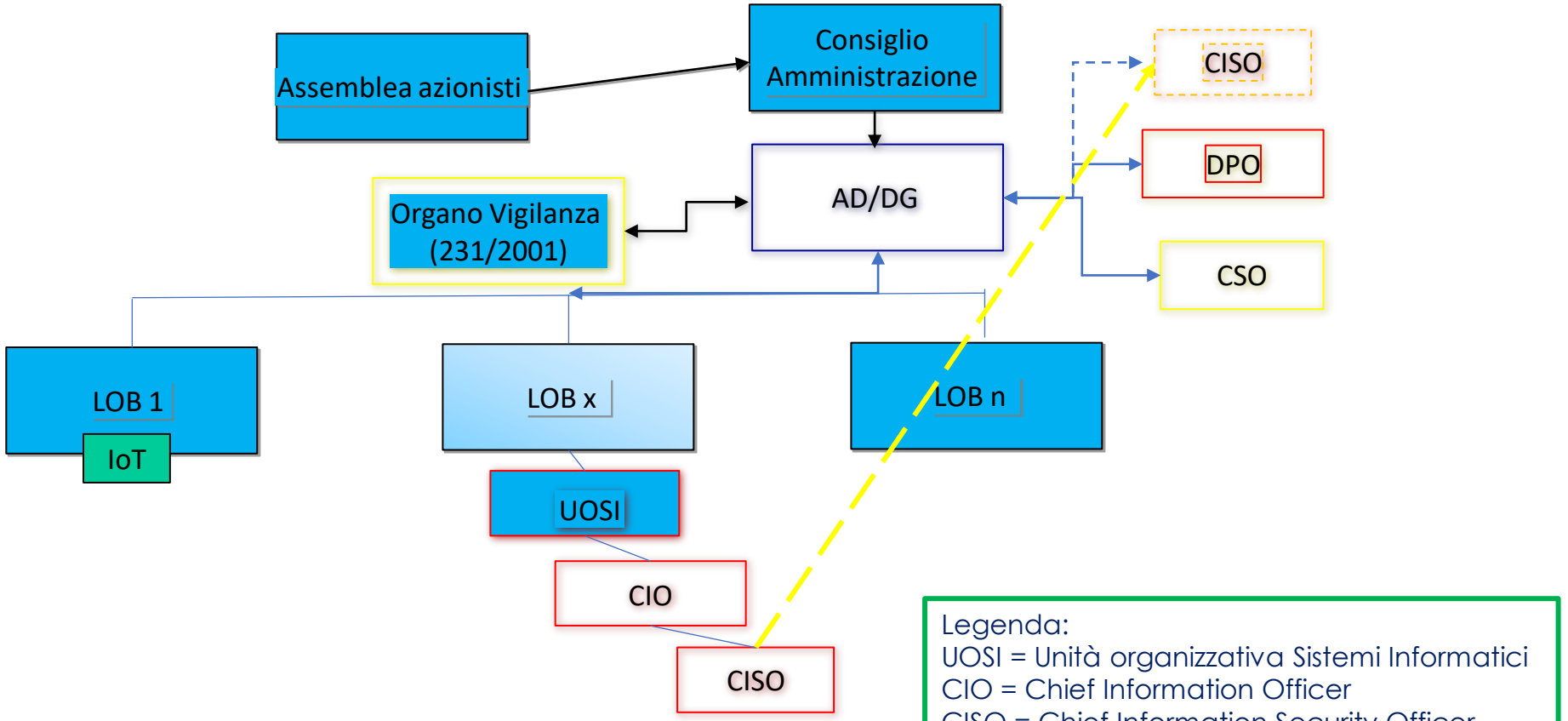
## CSaaS

## CyberSecurity as a Service

**Servizi di sicurezza digitale erogati in cloud**

- gestiti direttamente da chi si occupa della sicurezza digitale del Sistema Informativo “cliente”,
- Gestiti da Terze Parti, quali consulenti e società che li gestiscono in nome e per conto dei responsabili del Sistema Informativo del cliente
- CSaaS è un sottoinsieme dei MSS

# Organizzazione e sicurezza aziendale: il problema della “separation of diuties” all’interno dell’organizzazione




Legenda:
UOSI = Unità organizzativa Sistemi Informatici
CIO = Chief Information Officer
CISO = Chief Information Security Officer
CSO = Chief Security Officer
DPO = Data Privacy Officer
LOB = Line of Business

# Dall'indagine ISSA-ESG 2021: fortemente sottovalutato il ruolo del CISO


- **Cybersecurity Skills Crisis Continues for Fifth Year, Perpetuated by Lack of Business Investment**
- **The cybersecurity profession remains systemically undervalued**
- **Being offered a higher compensation package is the main reason (33%) CISOs leave one organization for another.**
- **Human resources and cybersecurity teams need to align on business value**
- **Business and cyber leaders need to work together to improve organizational dynamics**
  - 29% of respondents said the security team's relationship with HR is fair or poor.
  - 28% said the relationship with line-of-business managers is fair or poor.
  - 27% of respondents said that the relationship with the board of directors is fair or poor.
  - 24% said the relationship with the legal team is fair or poor.
- "**There is a lack of understanding between the cyber professional side and the business side of organizations that is exacerbating the cyber skills gap problem**" said Candy Alexander, Board President, ISSA International.




ESG RESEARCH REPORT

The Life and Times of Cybersecurity Professionals 2021

Volume V

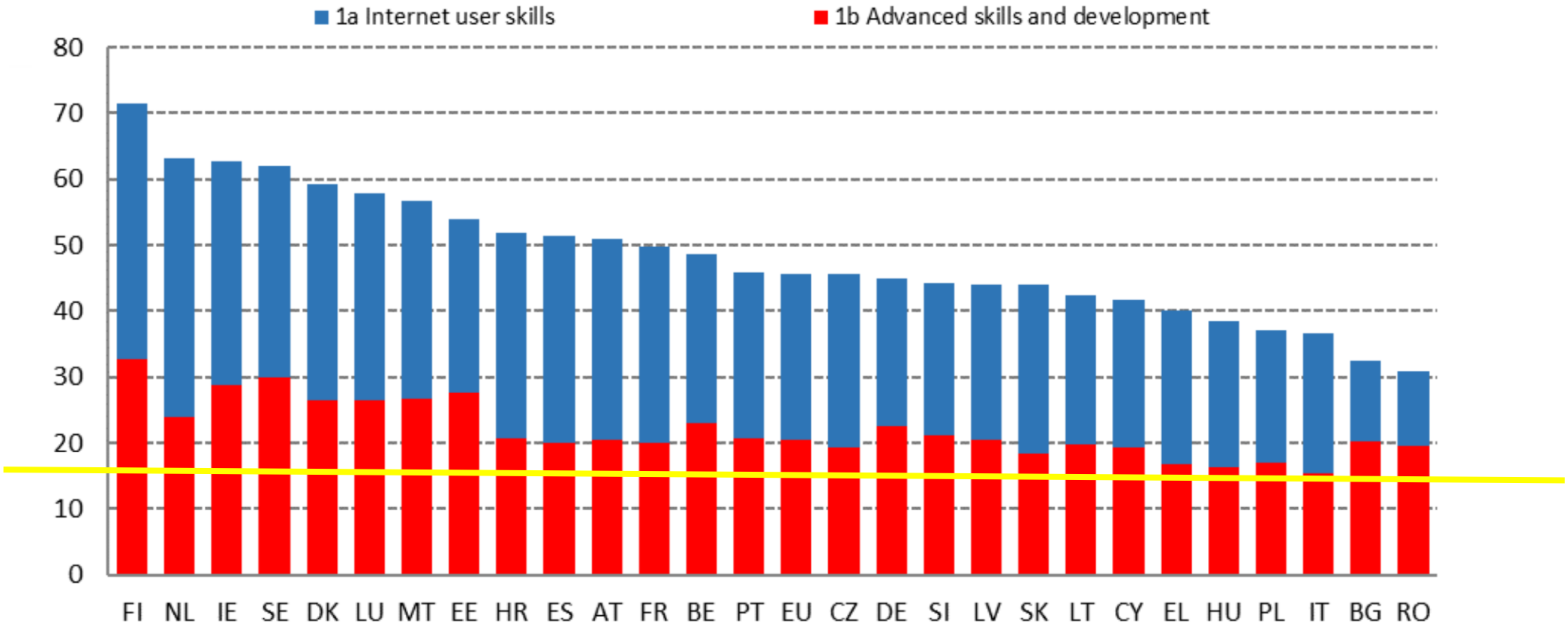
A Cooperative Research Project by ESG and ISSA

ISSA

By Jon Oltsik, Senior Principal Analyst and Fellow; and Bill Lundell, Director of Syndicated Research

July 2021

# DESI 2022: Competenze di base e specialistiche ICT (human capital)




*Source: DESI 2021, European Commission*

# I salari CIO e CISO in Italia e negli USA

## Per Italia da Page Group Italia (2022)

| JOB TITLE | <5 ANNI | 5-10 ANNI | >10 ANNI | % BONUS |
|---|---|---|---|---|
| Head Of Digital | 40.000-50.000 | 50.000-65.000 | > 65.000 | 10-20% |
| Programmatic Manager | 40.000-45.000 | 45.000-55.000 | > 55.000 | - |
| Digital Marketing Manager | 35.000-45.000 | 45.000-55.000 | > 55.000 | 10-15% |
| Creative Director | 35.000-45.000 | 45.000-55.000 | > 55.000 | - |
| Digital Performance Manager | 35.000-45.000 | 45.000-55.000 | > 55.000 | 10-15% |
| Digital Analyst | 35.000-40.000 | 40.000-50.000 | > 50.000 | - |

| SECURITY & GDPR | <5 ANNI | 5-10 ANNI | >10 ANNI | % BONUS |
|---|---|---|---|---|
| Chief Information Security Officer (Ciso) | 60.000-70.000 | 80.000-100.000 | >100.000 | 0-20% |
| Data Protection Officer | 55.000-65.000 | 70.000-80.000 | >80.000 | 0-20% |
| Security Manager | 50.000-55.000 | 55.000-70.000 | >70.000 | 0-20% |
| Gdpr & Data Governance | 45.000-55.000 | 60.000-80.000 | >80.000 | 0-20% |
| Cyber Security Officer | 45.000-50.000 | 50.000-60.000 | >60.000 | 0-20% |
| Cyber & Network Security Engineer | 35.000-45.000 | 45.000-60.000 | >60.000 | 0-10% |
| **CLOUD & INFRASTRUCTURE** | **<5 ANNI** | **5-10 ANNI** | **>10 ANNI** | **% BONUS** |
| Cloud & Infrastructures Manager | 50.000-65.000 | 65.000-75.000 | >75.000 | 5-15% |
| Cloud & Network Architect | 50.000-65.000 | 65.000-75.000 | >75.000 | 5-15% |
| System & Network Engineer | 35.000-45.000 | 45.000-55.000 | >55.000 | 5-15% |

## Per gli USA da Salary Guide 2023 di Robert Half

| Title | 25th percentile | 50th percentile | 75th percentile |
|---|---|---|---|
| Chief Information Officer (CIO) | $183,250 | $222,500 | $267,250 |
| Chief Information Security Officer (CISO) | $165,500 | $200,250 | $243,250 |
| Chief Technology Officer (CTO) | $160,250 | $198,750 | $236,750 |
| Vice President of Information Technology | $154,750 | $187,000 | $215,750 |
| IT Director | $130,250 | $159,250 | $189,500 |

### Salary percentiles

Starting salaries can vary greatly depending on a job candidate's experience and expertise, as well as company size and market demand for the role. That's why we separate them into percentiles in the tables above, based on the following candidate descriptions.

**25th**

New to the role, with little or no experience; requires more than casual instruction or supervision to perform day-to-day duties

**50th**

Has the experience to consistently perform core responsibilities without direct supervision; very comfortable with processes and subject matter associated with the role

**75th**

Value to the organization goes far beyond the ability to perform normal job duties; has rare qualifications that enable consistent contribution in unique ways; ready for next career level when available

# Tavola Rotonda CIO – CISO

**Coordinata da Marco Bozzetti e Pasquale De Martino:**

- **Marco Armoni**, SOC Manager - Lutech e componente del Comitato Scientifico AIPSI
- **Alessio Ferraro**, System Administrator e responsabile cybersecurity Fondazione Lucio Sciutto
- **Massimo Marabese,** Group Chief Information Officer di CellularLine Group
- **Gianluca Minieri**, ICT Alstom
- **Angelo Salice**, Security Manager SoftLab DIGI Spa e Consigliere AIPSI
- **Roberto Zanna,** Temporary ICT and Digital Manager