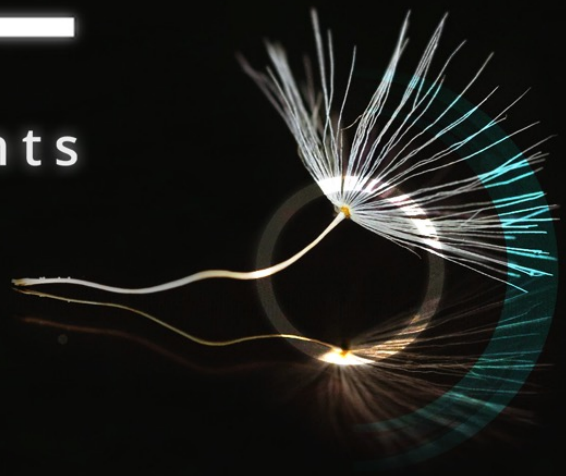
S2E

business & technology consultants



CYBERSECURITY ADVISORY & COMPLIANCE

Rel. 2305 – Distribution External

CSA&C
Cybersecurity Advisory & Compliance

CSA&C- PERIMETRO E STRATEGIA PROGETTUALE

VALORE AGGIUNTO DELL'OFFERING E DEL TEAM

- Competenza ed **esperienza pluriennale**
- Capacità di **analisi indipendente**
- Progetti e servizi **adeguati al contesto specifico**
- Ambito **globale** cybersecurity & compliance
- **Visione ampia e strategica** sui temi della sicurezza informazioni
- Definizione **processi operativi** cybersecurity
- Indirizzamento soluzioni specialistiche tramite **partner interni**
- **Training on demand**, frontale o tramite piattaforme dedicate
- **Coaching** … cosa deve fare un CISO/DPO/Privacy Officer?

CSA&C
Cybersecurity Advisory & Compliance

PERIMETRO DI INTERVENTO (WHAT)

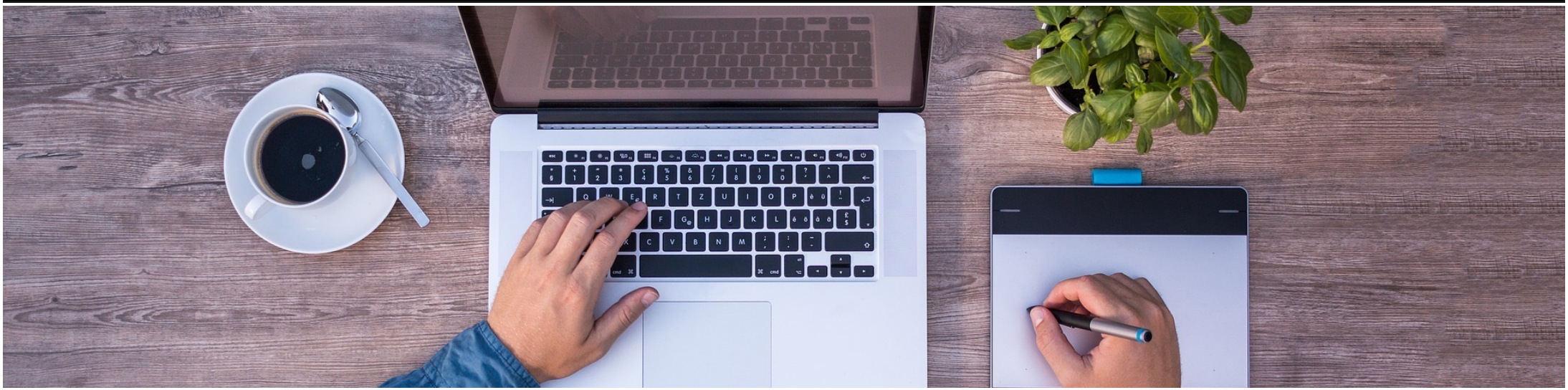
S◦2DE

Cybersecurity Advisory	Analisi del rischio ICT e pianificazione interventi di miglioramento postura cybersecurity
	Assessment cybersecurity rispetto ai principali framework (ISO27001, NIST CSF, CIS)
	Assessment cybersecurity per PMI
	Supporto definizione percorso di certificazione ISO/IEC 27001
	Assessment sicurezza di dettaglio rispetto ai singoli processi cybersecurity
	Definizione policy, procedure e processi cybersecurity
	CISOaaS, supporto al CISO
	Definizione processo di gestione degli incidenti di sicurezza informatica
	Business Continuity & Disaster Recovery Plan
	Miglioramento security supply chain
	Riduzione del rischio legato al fattore umano
	Integrazione OT Security (ISA/IEC62443)
	Cloud Security (ISO 27017, CSA STAR)
	Software Security (OWASP, WASC)
	Training frontale o tramite piattaforme dedicate

PERIMETRO DI INTERVENTO (WHAT)

Data Protection Advisory	Gap analysis & percorso di conformità GDPR
	DPOaaS
	Privacy Officer support
	Training
Compliance normativa	Adeguamento alle normative risk based
	NIS ed evoluzione NIS2
	Cyber Resilience Act
	Strategia Cybersecurity Nazionale
	Settore finance (EBA, DORA, Circ 285 Banca d'Italia, Tiber-IT, IVASS
	Misure minime di sicurezza AGID per la Pubblica Amministrazione
	Audit di conformità (processi di sicurezza, security by design)

CSA&C: I PRINCIPALI SERVIZI OFFERTI



ICT Risk Assessment
CISO as a Service
Business Continuity Planning
Human Cyber Risk Defense
Supply Chain Security

CSA&C
Cybersecurity Advisory & Compliance

01 SCENARIO → 02 DESIGN → 03 SERVICE

FRAMEWORK ISO27001:2022

Standard internazionale ISO

93 controlli di sicurezza suddivisi in **4 aree tematiche**

- persone (8)
- fisici (14)
- tecnologici (34)
- organizzativi (37)

5 attributi dei controlli

- **Tipo di controllo**: preventive, detective, corrective
- **Proprietà di sicurezza delle informazioni**: Confidentiality, Integrity e Availability
- **Concetti di cybersecurity**:
  - Identify, Protect, Detect, Respond e Recover
- **Capacità operative**:
  - Governance, Asset management, Information protection, Human resource security, Physical security, System and network security, Application Security, Secure configuration, Identity and access management, Threat and vulnerability management, Continuity, Supplier relationships security, Legal and compliance, Information security event management e Information security assurance
- **Domini di sicurezza**: Governance and ecosystem, Protection, Defence e Resilience

STRATEGIA CISO AS A SERVICE

S·2·E

RACCOLTA INFORMAZIONI

Organizzazione

Business e cultura aziendale

Stakeholder

ANALISI STAKEHOLDER

Organizzazione ICT

Business owner

Supply chain

REVIEW ANALISI DEL RISCHIO

Metodologia

Framework cybersec

Piano interventi

Efficacia misure di sicurezza

SECURITY ROADMAP

Priorità

Budget

Risorse disponibili

MISURAZIONE EFFICACIA

Misure

Trend

Key Perf Indicators

COMUNICAZIONE RISULTATI

Report Top Management

Dashboard

Coaching

Training

BUSINESS CONTINUITY PLANNING

Metodologia di conduzione BIA (Business Impact Analysis) basata sugli standard:

- ISO 22301:2012 “Societal security— Business continuity management systems”
- NIST SP800-34 Rev.1 “Contingency planning guide for federal information systems”

Fasi del progetto:

- Schedulazione interviste con i Referenti di Business owner dei Processi aziendali
- Somministrazione dei questionari ai Referenti di Business (insieme a referenti ICT)
- Attività di analisi e conclusioni finali tramite tool
- Deliverables di progetto: BIA report con Executive Summary

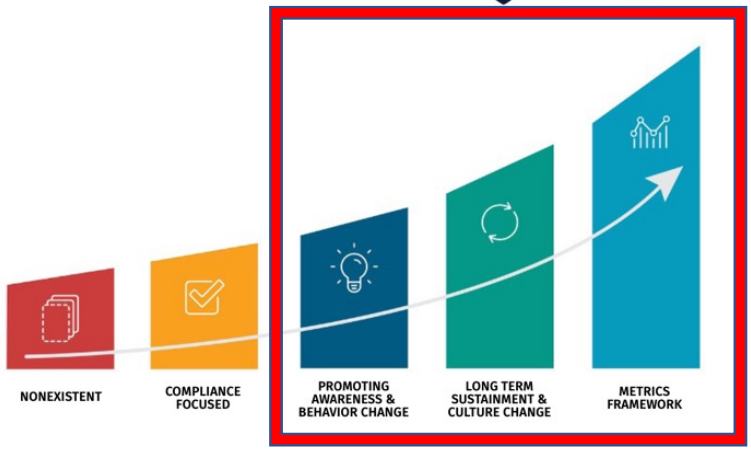
HUMAN CYBER RISK DEFENSE

S·2·E

- Security awareness evaluation
- Supporto nella definizione delle campagne anti phishing
- Security Culture improvement
- Formazione frontale o tramite tool
- Targeted attacks simulation (in partnership con ethical hacking team)
- Miglioramento del livello di maturità
- Riduzione del rischio legato al fattore umano

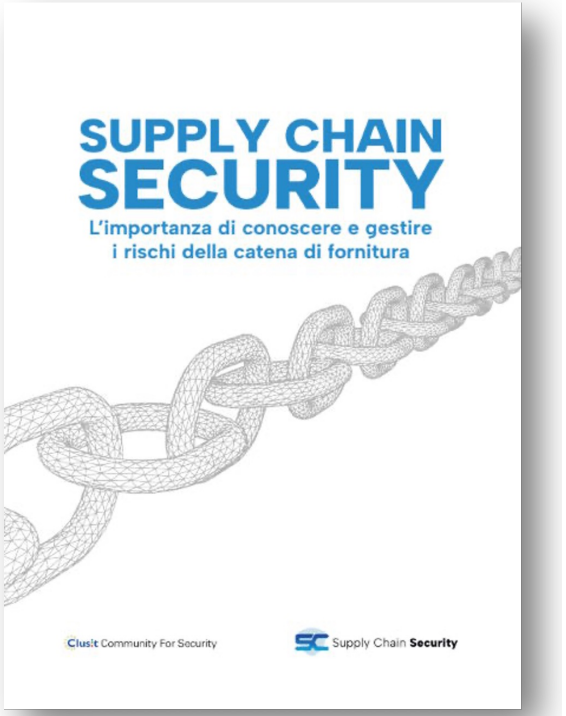
KnowBe4
Human error. Conquered.

Cyber Guru



Rischi principali

- Servizi cloud
  - Cloud storage, vulnerabilità delle piattaforme utilizzate
- Ciclo di sviluppo del software
  - Attacchi a repository
- Software di mercato ed open source
  - Patch Tuesday, CMS
- App per dispositivi mobili
  - App presenti su store ufficiali che distribuiscono malware
- Accesso remoto
  - Managed Service Provider, ransomware



GAP ANALYSIS GDPR

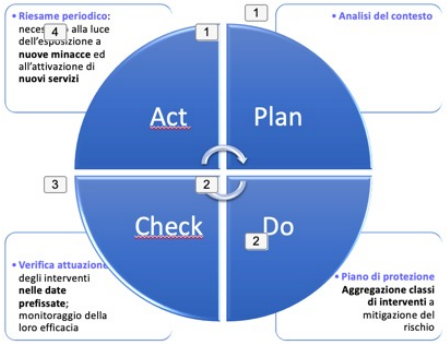
S·2·E

CAPO III - Diritti dell'interessato

- *Informazioni Ed Accesso Ai Dati Personali*
- *Diritto All'oblio*
- *Diritto Alla Limitazione Del Trattamento*
- *Portabilità Dei Dati*

CAPO IV - Titolare del trattamento e responsabile del trattamento

- *Responsabilità Del Titolare*
- *Privacy By Design/Default*
- *Contitolarità Del Trattamento*
- *Responsabili Esterni E Catene Di Fornitura*
- *Sicurezza Del Trattamento*
- *Registri Delle Attività Di Trattamento*
- *Data Breach Notification*
- *Data Protection Impact Assessment*
- *Data Protection Officer*



CAPO V - Trasferimento dati verso paesi terzi

- *Trasferimento Soggetto A Garanzie Adeguate*

CAPO VIII - Mezzi di ricorso, responsabilità e sanzioni

- *Rappresentanza Degli Interessati*
- *Sanzioni*

Approccio multidisciplinare (normativa,legale, misure di protezione)

COMPLIANCE PRINCIPALI NORMATIVE CYBERSECURITY

S◦2◗E

Normativa e tipologia	Ente di emanazione	Data di pubblicazione	Ambito	Settore	Data ultima prevista per l'adeguamento
Circolare 285 (40 aggiornamento	Banca d'Italia	2/11/2022	Disposizioni di vigilanza per le banche	Bancario	30 giugno 2023
Regolamento assicurativo	IVASS	2/8/2018	Regolamento recante disposizioni in materia di distribuzione assicurativa e riassicurativa	Assicurativo	Corrente
Linee guida Tiber IT	Banca d'Italia, Consob, IVASS	Agosto 2022	Threat Intelligence Based Ethical Red-Teaming – Italia	Bancario	Corrente
Regolamento DORA Digital Operation Resilence Act "	Parlamento e Consiglio Europeo	27/12/2022	Regolamento relativo alla resilienza operativa digitale per il settore finanziario	Finanziario	17 Gennaio 2025
Regolamento GDPR	Parlamento e Consiglio Europeo	27/4/2016	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	Tutti	Corrente
Direttiva NIS2	Parlamento e Consiglio Europeo	14/12/2022	Direttiva (ue) 2022/2555 del parlamento europeo e del consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione	Vari settori (vedi slide successiva)	18 ottobre 2024

STRATEGIA DI INTERVENTO

S·2·E

INPUT

- Attività
- Obiettivi
- Processi
- Attori
- Contratti

- Contesto operativo
- Articoli specifici normativa

- Misure di sicurezza da attuare
- Risorse (personale ed economiche)
- Priorità

- Informazioni raccolte

OUTPUT

- Applicazioni
- Dipendenze
- Catena di fornitura
- Vincoli normativi

- Postura corretta
- Inadeguatezza controlli
- Non conformità

- Percorso di conformità condiviso
- Piano di mitigazione dettagliato

- Metodologia
- Punti di attenzione


S2E
business & technology consultants
solutions2enterprises.com