Trend innovativi della sicurezza digitale in Italia

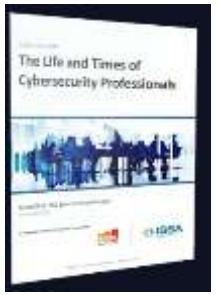
Marco R. A. Bozzetti

Presidente AIPSI

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

AIPSI, Associazione Italiana Professionisti Sicurezza Informatica

- Associazione apolitica e senza fini di lucro
- **Capitolo Italiano** di **ISSA**, Information Systems Security Association, (www.issa.org) che conta >>12.000 Soci, la più grande associazione non-profit di professionisti della Sicurezza ICT nel mondo
- **Obiettivo principale**: aiutare i propri Soci nella **crescita professionale** → competenze →carriera e crescita business
  - Offrendo ai propri Soci **servizi qualificati** per tale crescita, che includono
    - Convegni, workshop, webinar sia a livello nazionale che internazionale via ISSA
    - ISSA Journal
    - Rapporti annuali e specifici; esempi:
      - Rapporto annuale **OAD** nel nuovo sito **https://www.oadweb.it**
      - **ESG ISSA Survey** "The Life and Times of Cyber Security Professionals"
    - Concreto supporto nell'intero ciclo di vita professionale, con formazione specializzata e supporto alle certificazioni, in particolare eCF Plus (EN 16234-1:2016)
    - Collaborazione con varie Associazioni ed Enti per eventi ed iniziative congiunte
    - Gruppo Specialistico di Interesse **CSWI, Cyber Security Women Italy**, aperto a tutte le donne che in Italia operano a qualsiasi livello nell'ambito della sicurezza digitale (anche non socie AIPSI)



OAD, Osservatorio Attacchi Digitali in Italia

2018

10 anni di indagini via web sugli att… …stemi informatici in I…

OAD 2019 è iniziato con la ricerca di sponsor e la messa a punto del questionario on line.
A breve disponibile on line via web: *compilatelo!*
https://www.oadweb.it

Il contesto della sicurezza digitale e nuove logiche di approccio

- Crescente pervasività dell'ICT in ogni attività e in ogni dispositivo
- Attacchi digitali sempre più critici per il loro impatto sul business
- Cybersecurity sempre più importante
- Fino ad oggi le **misure tecniche ed organizzative di sicurezza digitale**, **dal costo crescente**, si articolano in:
  - misure di prevenzione
  - misure di contrasto
  - misure di back up e ripristino
- ***Ma sono sufficienti ed efficaci?***
  - Sono necessarie ma non sufficienti, con una continua e costosa rincorsa per far fronte alle nuove vulnerabilità e ai nuovi attacchi, che in molti casi sono comunque a favore degli attaccanti
- Molti esperti, a livello mondiale, ritengono che non si debba più spendere prevalentemente per tali misure (ma sono ancora necessarie), ma investire di più in **misure per bloccare e reprimere l'hackeraggio/cyber crime**, riducendo fortemente i loro alti guadagni con pochissimi rischi
  - *… If they [vulnerabilities] are dense, then finding and fixing one more is essentially irrelevant to security and a waste of the resources spent finding it." (da Dan Geer)*
  - *But if you care about systemic security […] don't chase and fix vulnerabilities, […] design a system around fundamentally stopping routes of impact. (da Bas Alberts)*

OAD 2018: dati Polizia Postale - 1

C.N.A.I.P.I.C. Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

Protezione strutture critic	gen – 31 dic 201	gen – 31 dic 2016	Differenza %
Attacchi rilevati	1032	844	**22,27%**
Alert diramati	31524	6721	**369,04%**
Indagini avviate	72	70	**2,86%**
Persone arrestate	3	3	**0,00%**
Persone denunciate	1316	1226	**7,34%**
Perquisizioni	73	58	**25,86%**
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	83	85	**-2,35%**

Indagini/ attacchi 6,89%

Indagini/ attacchi 8,29%

Arresti/ denunce 0,23%

Arresti/ denunce 0,24%

OAD 2018: dati Polizia Postale - 2

Financial Cyber Crime

Financial Cyber Crime	1 gen – 31 dic 2017	1 gen – 31 dic 2016	Differenza %
Transazioni Fraudolente Bloccate in €	€ 20.839.576,00	€ 16.050.812,50	**29,84%**
Somme Recuperate	€ 862.000,00	=	
Arrestati	25	25	**0,00%**
Denunciati	2851	3772	**-24,42%**

Arresti/ denunce 0,88%

Arresti/ denunce 0,66%

Cyber Terrorismo

Cyber Terrorismo	1 gen – 31 dic 2017	gen – 31 dic 2016	Differenza %
Arrestati	4	2	**100,00%**
Denunciati	18	9	**100,00%**

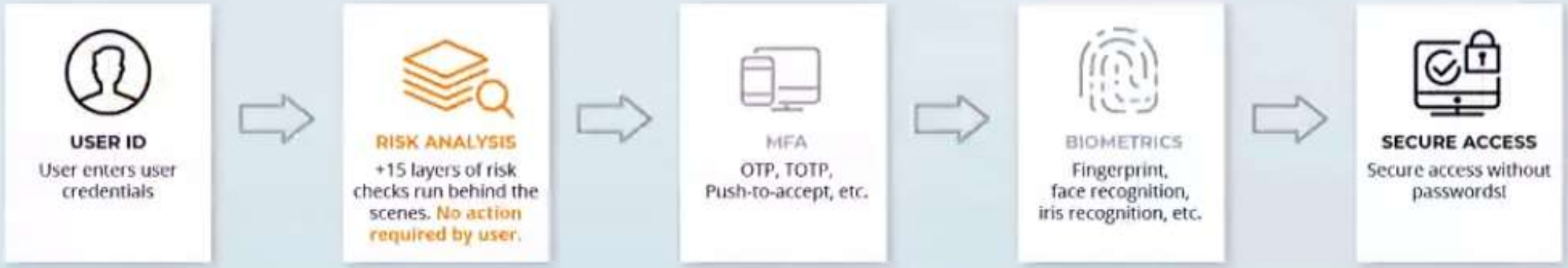
Arresti/ denunce 22%

Arresti/ denunce 22%

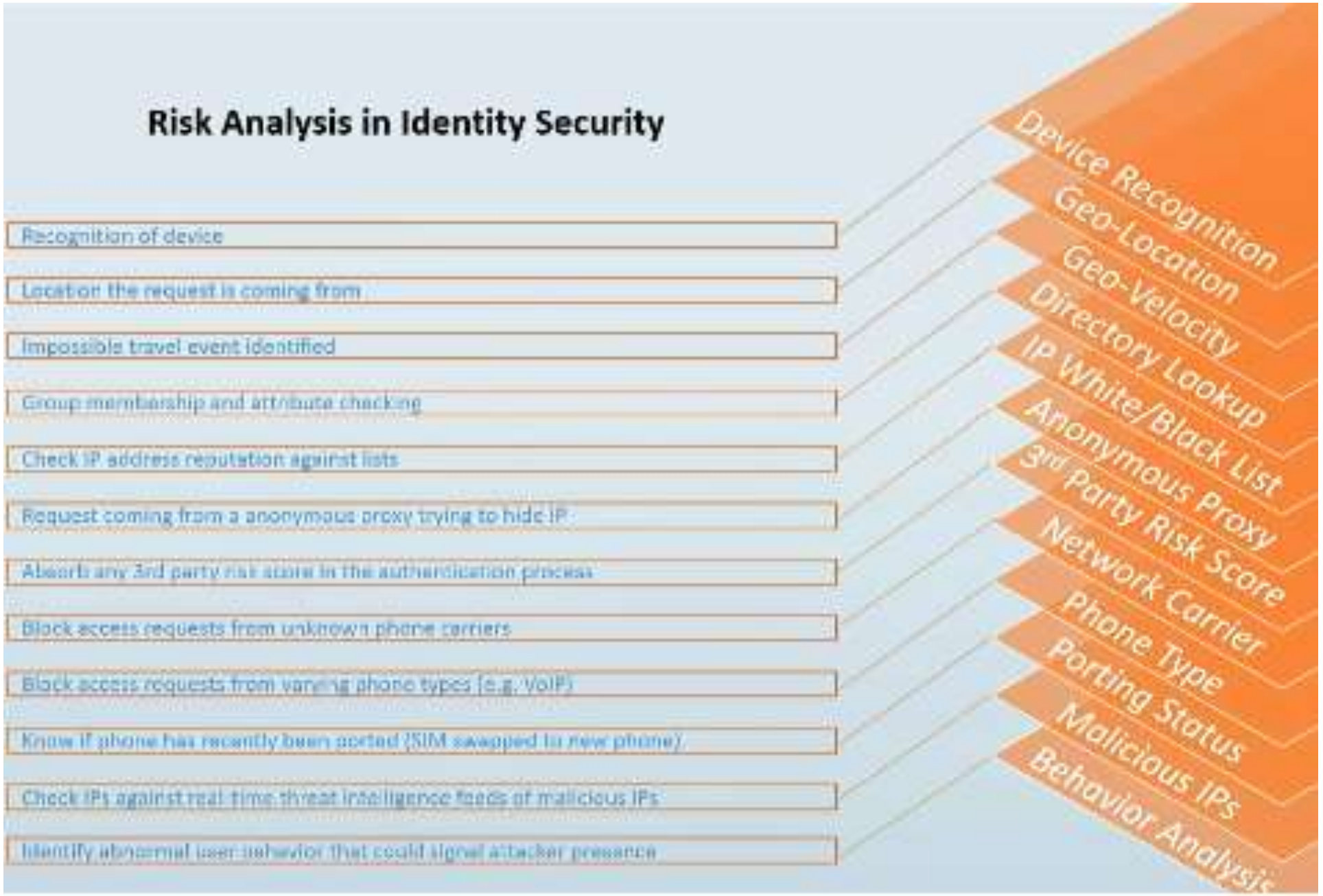
2019: un anno di novità per la sicurezza digitale (elenco non esaustivo)

- **A livello tecnico**
  - Significative innovazioni o consolidamento di tecniche che iniziano realmente a consoliidarsi e a diffondersi
    - Nuove logiche e tecniche di autenticazione: out of band, passwordless, etc.
    - Nuove logiche e tecniche di autorizzazione: Diameter, NGAC, NISTIR 8112, etc.
    - Intelligenza artificiale (AI), sistemi esperti, machine learning
    - Analisi comportamentale sistemi e utenti : AI, logiche bayseniane, etc.
    - Crescente integrazione tra security e safety nell'ambito dei cyber physical system
    - Crescente integrazione ed innovazione nei sistemi di monitoraggio e controllo
    - Nuove logiche ed ambienti di sviluppo sw: DevOps, leaning/agile programming, etc.
    - Blockchain: utilizzi al di fuori delle cripto valute, varie vulnerabilità, prevalenza soluzioni private (chiuse)
    - …….
- **A livello organizzativo**
  - ITIL 4, profonda evoluzione di ITIL 3/2011
  - COBIT 2019
  - Mancanza competenze e sensibilizzazione (soprattutto ai vertici) sulla sicurezza digitale
  - Crescita terziarizzazione servizi di sicurezza digitale
  - Impatto della gestione e della terziarizzazione della sicurezza digitale sulla struttura organizzativa
- **A livello normativo**
  - CyberSecurity Act europeo e nuovo ruolo Enisa
  - Impatto crescente compliance GDPR

Passwordless Authentication in Practice



Un esempio delle analisi a supporto dell'identificazione e autenticazione



Fonte: ISSA

DevOps: che cosa è

- **DevOps** (dalla contrazione inglese di *development*, "sviluppo", e *operations*, qui simile a "messa in produzione" o "*deployment*") è un metodo di sviluppo del software che punta alla comunicazione, collaborazione e integrazione tra sviluppatori e addetti alle *operations* dell'ICT.
- DevOps vuole rispondere all'interdipendenza tra sviluppo software e IT operations, puntando ad aiutare un'organizzazione a sviluppare in modo più rapido ed efficiente prodotti e servizi software
- Secondo il modello DevOps, i team dedicati a sviluppo e produzione non agiscono più separatamente. In alcuni casi, al contrario, i due team vengono fusi in un'unità in cui i tecnici sono attivi lungo tutto il ciclo di vita dell'applicazione, da sviluppo e testing a distribuzione e produzione, e acquisiscono una serie di competenze non limitate da una singola funzione.
- In alcuni modelli DevOps, anche i team dedicati a controllo della qualità e sicurezza spesso sono coinvolti più direttamente nelle fasi di sviluppo e gestione in tutto il ciclo di vita dell'applicazione.
- Quando in un team di DevOps la sicurezza è il punto focale di tutti, a volte prende il nome di DevSecOps.
- I team si affidano all'automatizzazione per velocizzare processi manuali che sono da sempre lenti.

Fonte: AWS e Wikipedia

Uso crescente di tecniche di blockchain

- **Notarization Journal**:
  - Consenso sulle modifiche ad un registro in presenza di una autorità centrale
- **Distributed Ledger Technology** (DLT)
  - sistemi che permettono ai nodi di una rete di raggiungere il consenso sulle modifiche di un registro distribuito in assenza di fiducia e senza la presenza di un ente centrale
- **Blockchain**
  - tecnologia in cui il registro distribuito è strutturato come una catena di blocchi contenenti transazioni - alla base del Bitcoin,
- **Internet of Value**
  - una rete digitale di nodi che si trasferiscono valore; in assenza di fiducia, un sistema permette di raggiungere il consenso sulle modifiche di un registro distribuito delle transazioni

Principali vulnerabilità della blockchain, causa di vari attacchi

- **A livello di rete:** DoS/DDoS, Sybil attack (allo stesso nodo vengono assegnate molte diverse identità), Eclipse attack (offuscare i nodi sani da uno malevolo)
- **A livello d'utente finale:** sfruttando le vulnerabilità del dispositivo d'utente (end point vulnerability) e botnet
- **A livello delle chiavi crittografiche:** furto chiavi (con varie tecniche, in primis social engineering)
- **Attacchi a livelli di maining:** sfruttando vulnerabilità della piattaforma, ad esempio per bachi di codice, double-spending attack (si spende per due volte la stessa somma di cripto-valuta, sfruttando malfunzionamenti, in particolare del client)
- **Rischi dei vendor e delle Terze Parti coinvolte:** Blockchain integration platforms, Payment processors, Wallets, Fintech, Blockchain payment platforms, Smart contracts
- **Numero dei partecipanti**, ai vari livelli, alla blockchain. La blockchain (soprattutto pubblica) può considerarsi affidabile se e solo il numero di attori è veramente elevato: regola del 51%
- Accordo tra **più mainer disonesti**
- Più blocchi ha la stessa catena, più capacità elaborativa e di storage è richiesta più lunghi sono i tempi di risposta per transazione (10 minuti …) → **centralizzazione in pochi potenti nodi** …
- Utilizzo di **attacchi indipendenti dalle tecniche di block chain**

Tipi di blockchain

- **Public blockchain**:
  - Completamente distribuita – replicata in ogni nodo
  - Ogni nodo può inserire validare ed inserire blocchi
  - La proof of work (POW) ne garantisce la robustezza
  - Non richiede una autorità centrale che controlla la correttezza delle applicazioni
- **Private blockchain**:
  - Prevede una autorità responsabile p[illegible] la correttezza delle operazioni
  - I validatori (mainer) sono autenticati dalla autorità
  - La struttura non è necessariamente distribuita su tutti i nodi
  - I nodi non-validatori possono essere autenticati o meno
- **Consortium blockchain**:
  - Blockchain condivisa tra più organizzazioni/autorità

Prevalentemente usata per cripto valuta
Hanno subito vari e significativi attacchi

Le più usate in ambito aziendale per diversi settori: logistica, documentale, etc.

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

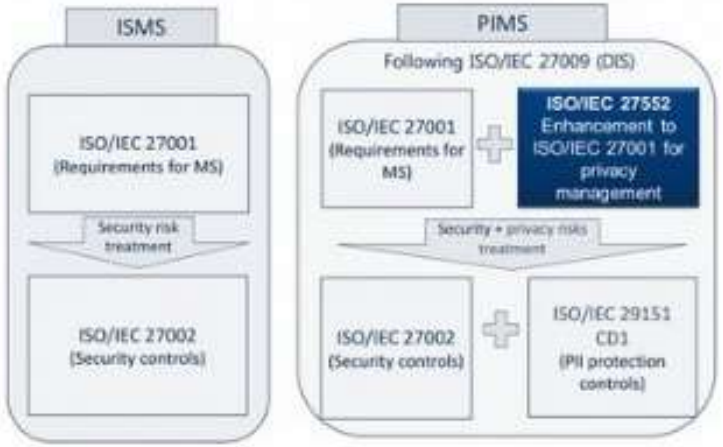
Vulnerabilità e attacchi 5G, rete wireless x 1K più potente del 4G: upload fino a 10Gbps e latenza < 5 ms

- Distinguere una prima fase di adozione del 5G dal suo consolidamento.
- Nella prima fase soluzioni 5G (URLLC, Ultra-Reliable Low Latency Communications) si affiancheranno alle reti 3 e 4 G, e probabilmente rimarranno le stesse vulnerabilità di queste
- Seri problemi, anche evidenziati dal Parlamento europeo, sui sistemi 5G cinesi, preminenti sia negli US che in Europa, per possibili ”backdoor“ inclusi in questi prodotti, che consentirebbero ai fornitori e alle autorità cinesi di avere un accesso non autorizzato ai dati e alle telecomunicazioni dei loro clienti (si rammenta che la Cina è una dittatura comunista)
- Esempi dei principali attacchi previsti anche per 5G, basati su vulnerabilità dei protocolli di rete:
  - **Torpedo,** TRacking via Paging mEssage DistributiOn
  - **Piercer,** Persistent Information ExposuRe by the CorE network
  - **IMSI-Cracking** (medesimo obiettivo di Piercer, scoprire l’identificativo di rete del sistema attaccato)
  - **aLTEr:** creazione di una cella che opererebbe come Mitm

Nuove ISO 27001 - 27552

ISO/IEC 27552, Enhancement to ISO/IEC 27001 for privacy management

- Norma in lavorazione (1st CD) con completamento previsto per aprile 2019
- Documento non autoconsistente che segue le indicazioni della ISO/IEC 27009
- Richiamo dell'approccio verso un PIMS
- Forte attenzione dedicate ai controlli
- Partecipazione attiva del WP 29 e di diverse autorità europee (FR, IT in primis)



ISO/IEC 27552 development timeline

December 2018

Draft International Standard (DIS) expected to be made available.

Open for public comment for three months.

June 2019

Final Draft International Standard (FDIS) expected to made available.

Q4 2019 – January 2020

Final Standard expected to publish.

Intelligenza Artificiale e sicurezza digitale

- AI, con le sue varie declinazioni machine learning, sistemi esperti, etc., sta entrando in vari settori ed aspetti della sicurezza digitale:
- Supporto alla automazione di vari processi operativi della sicurezza digitale: gestione incidenti, allarmi, problemi, etc.
  - Correlazione e selezione di eventi (es log di utenti e sistemi ICT).
- Analisi dei rischi e analisi comportamentale
- Analisi dei possibili scenari e supporto decisionale
- Associazione con modelli e calcoli bayseniani

Il problema di fondo: fino a che punto possiamo lasciare decisioni attuative a sistemi di AI?

10 Trend nell'AI applicata alla Cybersecurity

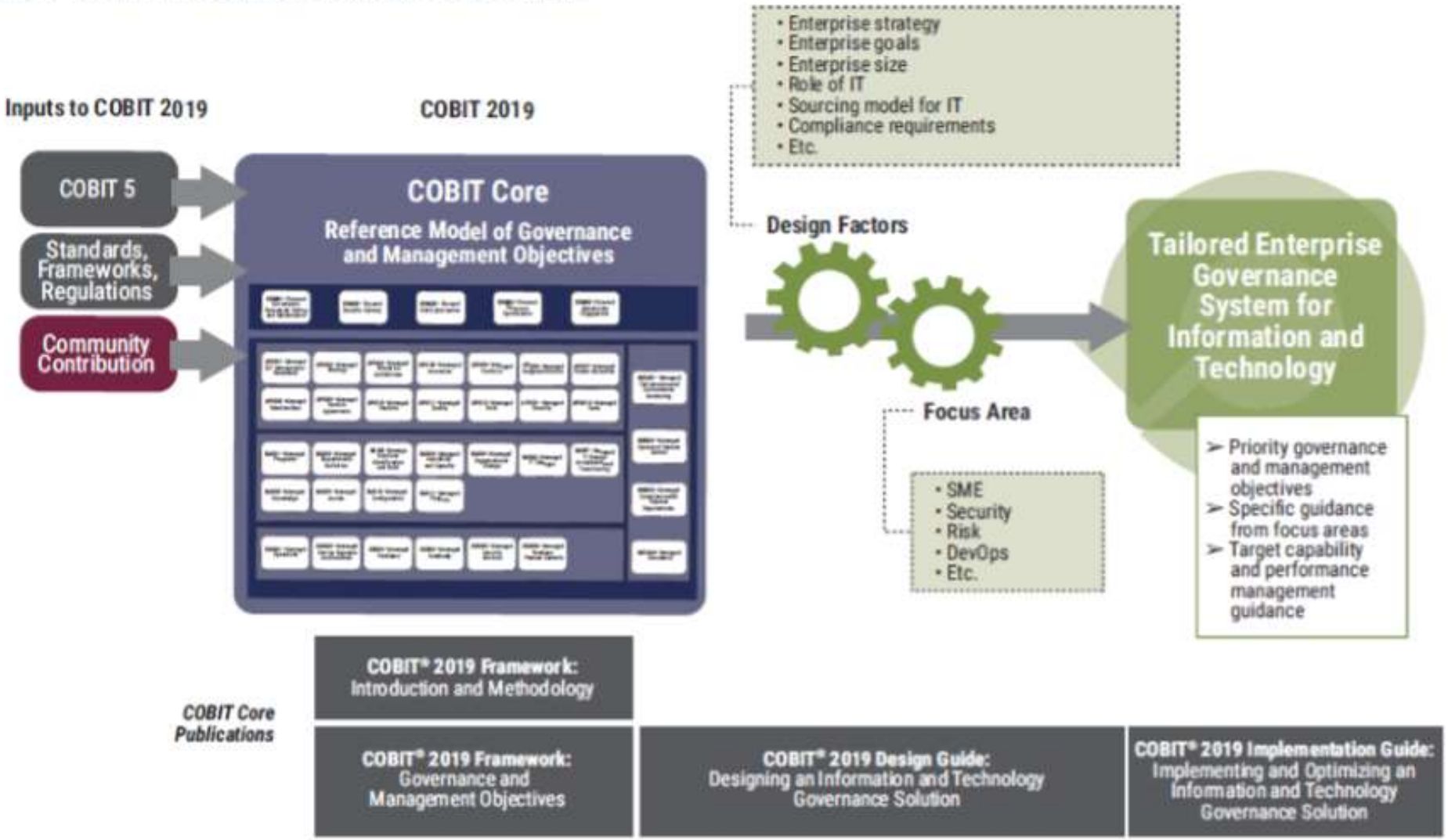
- Responding to Ransomware
- Combining Application Development and Cybersecurity
- Using Deep Learning to Detect DGA-Generated Domains
- Detecting Non-Malware Threats
- Adaptive Honeypots and Honeytokens
- Gaining a Better Understanding of How Neural Networks Work
- Employing Capsule Networks
- Deep Reinforcement Learning
- Protecting the IoT
- Predicting the Future

Fonte: M. Armoni, AIPSI

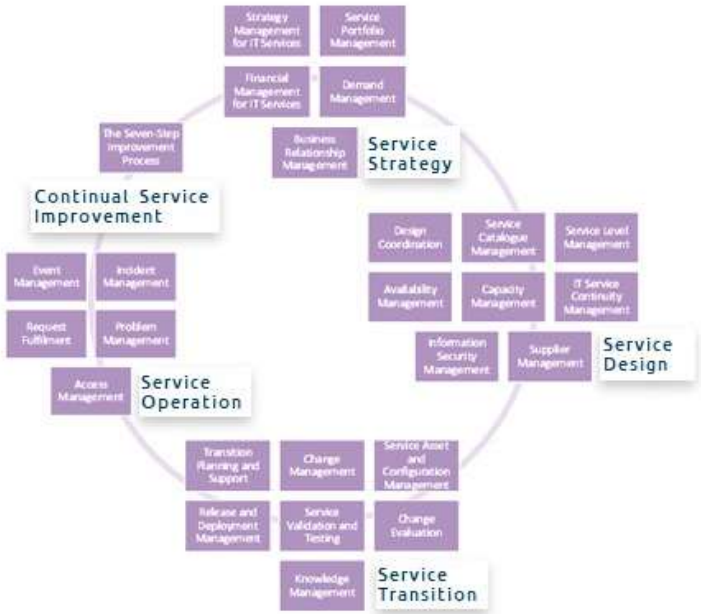
aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

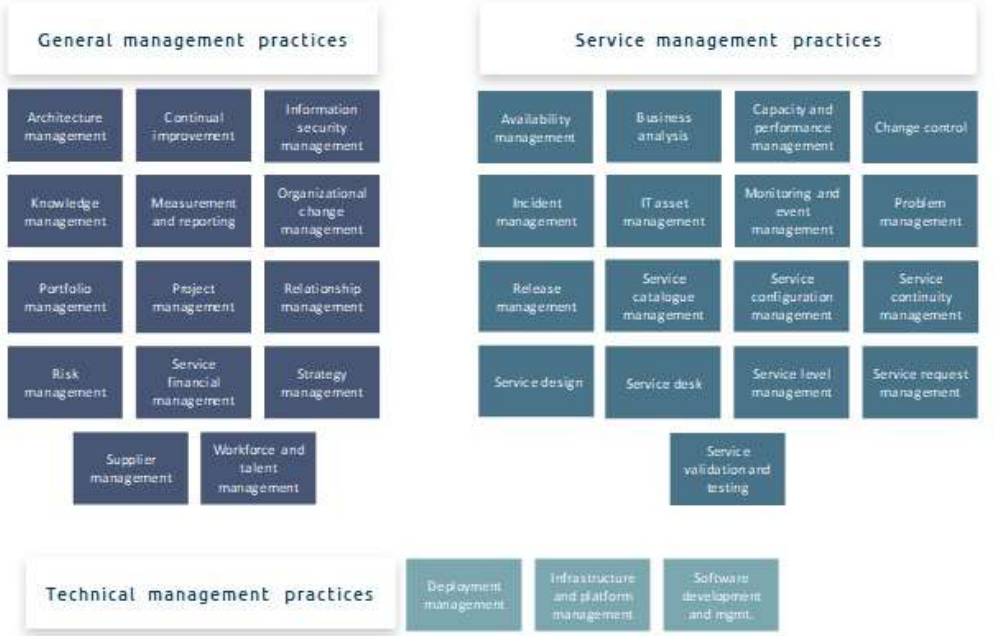
COBIT OVERVIEW

COBIT 2019 PRODUCT ARCHITECTURE



ITIL 4: dai processi alle pratiche





ITIL® V3
26 service lifecycle processes

ITIL® 4
34 management practices

yasm.com/wiki/en/ | YaSM® – Yet another Service Management Model

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

Cybersecurity Act dell'UE - 1

- A fianco della **Direttiva Europea NIS del 2016**, trasposta in Italia dal D.Lgs. 65/2018 che fa riferimento a carrier TLC e a infrastrutture critiche, ed istituisce anche il CSIRT, il Gruppo di intervento per la sicurezza informatica in caso di incidente, al posto dei CERT, è stato emanato il **Regolamento UE 2019_881 *Cybersecurity Act*** che dettaglia un ulteriore quadro per il rafforzamento della sicurezza cibernetica dei sistemi informatici e delle reti in ogni paese dell'Unione Europea.
- Questo Regolamento è stato pubblicato in Gazzetta Ufficiale il 7 giungo 2019 ed **entrerà in vigore il 27 giugno 2019**
- Esso costituisce la basa della strategia UE per la cybersecurity, che mira a rafforzare la resilienza dell'Unione agli attacchi informatici, a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi e ad accrescere la fiducia dei consumatori nelle tecnologie digitali.
  - "Le persone e le imprese devono sentirsi sicure nell'ambiente digitale; solo così potranno beneficiare appieno dell'economia digitale europea. La fiducia e la sicurezza sono fondamentali per il corretto funzionamento del nostro mercato unico digitale" - ***Andrus Ansip**, Vicepresidente e Commissario responsabile per il Mercato unico digitale.*
  - "Consolidare la cybersicurezza dell'Europa e accrescere la fiducia dei cittadini e delle imprese nella società digitale è una priorità assoluta dell'Unione europea. Credo fermamente che l'accordo raggiunto stasera non solo migliori la cybersicurezza complessiva dell'Unione ma sostenga anche la competitività delle imprese" - ***Mariya Gabriel**, Commissaria responsabile per l'Economia e la società digitali.*

Cybersecurity Act dell'UE - 2

- Il regolamento Cybersecurity Act si suddivide in due parti:
  - **Il nuovo ruolo di ENISA**
    - un mandato permanente per l'Agenzia (ora è limitato e scade il 2020)
    - un potenziamento di ruolo e di risorse
    - Il coordinamento di agenzie nazionali
  - L'introduzione di un **sistema europeo per la «certificazione» della sicurezza informatica dei dispositivi connessi ad Internet e di altri prodotti e servizi digitali**
    - Rivisitazione di schemi di certificazione/qualificazione della sicurezza digitale di dispostivi, sistemi, servizi ICT (tipo Common Criteria) e dallo schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (Decreto Del Presidente Del Consiglio Dei Ministri 30 Ottobre 2003)**,** attualmente in carico all' **Iscom**, Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, operante presso il Ministero dello Sviluppo Economico (http://www.isticom.it/)
      - Il regolamento prevede 3 livelli di certificazione diversi per sistemi con affidabilità di base, sostanziale, elevata.
    - La certificazione in oggetto è indirizzata a tutti i dispositivi e sistemi ICT o con parti ICT embedded, inclusi IoT, domotica, etc., e spinge per l'adozione della **security by design** e **by default**

I nostri riferimenti

- aipsi@aipsi.org
- www.aipsi.org
- www.oadweb.it

- m.bozzetti@aipsi.org

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA