ABI Lab

CERTFin

17.05.2023

EVOLVERE IN SICUREZZA
Nuovi strumenti per la resilienza operativa _

La resilienza digitale è la resilienza di tutta la banca

Il trend in atto è orientato verso i **servizi intrinsecamente digitali**

Richiedono il coordinamento con fornitori tecnologici

L'**IT** da strumentale è **divenuta strategica** e la Banca è divenuta **digitale**

La banca diviene i servizi digitali che offre

L' ICT è fattore abilitante dell'offerta finanziaria, tradizionale e innovativa

Sono sfide che richiedono **capacità specifiche** che permettano di **evolvere nelle difficoltà**

- condurre in continuo **analisi previsionali** sugli scenari di minacce e relativi impatti
- affrontare **combinazioni contemporanee di più scenari di incidente** incluse indisponibilità dei servizi sociali e infrastrutturali connessi con il proprio ecosistema
- modificare i propri processi e procedure operative con tempestività e flessibilità
    - prevedere gestire e attivare **catene alternative di approvvigionamento di beni e servizi** (supply chain).

rischi ICT = rischi di business

DORA

12/2019 - Avvio consultazione

09/2020 - Prima bozza del regolamento

12/2022 - Pubblicazione

01/2023 - Entrata in vigore

01/2024 - I° Emanazione RTS

07/2024 - II° Emanazione RTS

01/2025 – Applicazione del DORA

Si applica a oltre 20 categorie di soggetti(art. 2), complessivamente definiti **entità finanziarie**, fa cui

AZIENDE FINANZIARIE TRADIZIONALI (BANCHE, ASSICURAZIONI)

FORNITORI DI SERVIZI ICT E DI COMUNICAZIONE

ALTRE AZIENDE FINANZIARIE

- ISTITUTI DI PAGAMENTO E DI MONETA ELETTRONICA
- FONDI DI INVESTIMENTO
- INFRASTRUTTURE DI MERCATO
- FORNITORI DI SERVIZI DI CRIPTO ASSET O CROWDFUNDING

Obiettivi

- Conseguire un **livello comune** elevato di resilienza operativa digitale nel settore finanziario
- Definire **requisiti uniformi** per la sicurezza dei sistemi informatici e di rete che sostengono i processi commerciali delle entità finanziarie
- Garantire sicurezza, agilità e **continuità** dei servizi offerti sostenendo il continuo processo di digitalizzazione
- Adattarsi all' **evoluzione** degli scenari di rischio
- Rafforzare il livello di **resilienza ai rischi digitali**
- **Prevenire, contenere e ridurre** gli impatti in caso di incidenti

Attività a supporto dell'implementazione del DORA presso l'Osservatorio Continuity & Resilience

Attività di supporto alla implementazione del DORA

- Censimento dei **deliverable** richiesti (Policy, Piani, Processi, Framework, Strategie, Analisi, Registri, ….), descrivendo contenuti e metodi di **realizzazione e gestione**
- Comparazione differenziale rispetto alla preesistente normativa con evidenza degli elementi innovativi
- Checklist di alto livello sul grado di copertura requisiti Dora in azienda
- Raccolta **quesiti interpretativi** sul DORA
- **Monitoraggio** sullo sviluppo degli RTS del DORA

Gennaio 2024 - I° Emanazione RTS

- RTS on **ICT Risk Mng.** Framework
- RTS on Simplified ICT Risk Management Framework
- RTS on **Incident Reporting classification criteria**
- ITS on Register Template (informazioni su **contratti con fornitori** ICT)
- RTS on **ICT Services Policy**

Luglio 2024 - II° Emanazione RTS

- RTS on **Reporting of major incident**
- ITS on Incident **Reporting details**
- GL on **estimation of costs/ losses** from major ICT incidents
- RTS on **TLTP** Threat led penetration test
- RTS **on sub contracting elements**

Gennaio 2025

Feasibility Report on Incident Reporting EU Hub

Aggiornamento del **B**usiness **R**esilience **F**ramework affinché:

- indirizzi **tutti gli articoli del DORA** afferenti obblighi per le banche
- descriva **contenuti e metodi di realizzazione per i deliverable richiesti dal DORA**
- suggerisca **processi coerenti con DORA**
- Integri la gestione dei **requisiti di dettaglio esposti negli RTS**
- Proponga **misure per valutare il proprio grado di resilienza**
- Induca la adozione dei **principi di resilienza** del DORA **oltre il digitale**
- Preveda **guida** di lettura specifica **per le diverse funzioni aziendali**

La documentazione richiesta da DORA

Politiche / Strategie:

- di resilienza operativa digitale
- di continuità operativa e
- di continuità ICT
- di sicurezza dell'informazione
- per l'uso (e di uscita) di servizi prestati da fornitore terzo
- di Backup
- di comunicazione interna
- per i rischi informatici derivanti da terzi
- di uscita

Mappature:

- BIA
- Matrice di correlazione fra Funzioni commerciali, Ruoli, patrimoni informativi, risorse ICT
- Servizi ICT forniti da fornitori terzi
- Sistemi, i processi e le tecnologie ICT a supporto delle funzioni essenziali o importanti e tutti i pertinenti servizi, gestiti da fornitori terzi

Altro:

- Registro delle attività in caso di crisi
- Registro di informazioni su gli accordi contrattuali ICT
- Soglie di allarme e criteri di attivazione processi di risposta
- Stima dei costi e delle perdite annuali aggregati causati da incidenti gravi ICT

Piani e procedure:

- Di Continuità Operativa (preparazione, risposta, gesti di crisi/incidenti) e di risposta e ripristino ICT
- Di Audit , di Formazione e di Test (comprese procedure backup)
- Di Comunicazione (interna ed esterna)
- Di Uscita (dalle forniture di servizi)
- Per la gestione delle modifiche delle ICT ,
- Per i diritti di accesso fisico e logico ai patrimoni informativi
- DI Risoluzione (Remediation plan)
- Di Gestione e di segnalazione degli incidenti

WORK IN PROGRESS

Gap Analysis DORA – 285/EBA GL

ABI Lab

1 **Identificazione requisiti di interesse**

Sono stati individuati i requisiti del DORA rivolti alle entità finanziarie. Sono stati quindi esclusi i requisiti rivolti alle AEV.

2 **Confronto tra normative**

Ogni requisito del DORA è stato analizzato rispetto alla Circolare 285 e alle Disposizioni di Vigilanza, identificando i requisiti già presenti del tutto o in parte nella normativa pregressa.

- Requisito presente in modo completo: solo azioni marginali di allineamento
- Requisito presente in modo parziale : Eseguire gap analysis rispetto a quanto già implementato
- Requisito non presente
  Nuovo requisito da implementare

In totale sono stati analizzati 236 requisiti del DORA	59 punti di confronto	96 punti di confronto	81 punti di confronto
Capo II – Gestione dei rischi informatici	43	39	27
Capo III – Gestione, […] degli incidenti informatici	11	5	12
Capo VI – Test di resilienza operativa digitale	0	5	26
Capo V – Gestione dei rischi informatici derivanti da terzi	5	47	10
Capo VI – Meccanismi di condivisione delle informazioni	0	0	6

CERTFin

Checklist sui requisiti DORA

• **CAPO II:** Gestione dei rischi informatici	(artt. 5-14)	48 domande
• **CAPO III:** Gestione, classificazione e segnalazione degli incidenti informatici	(artt. 17-19)	5 domande
• **CAPO IV**: Test di resilienza operativa digitale	(artt. 24-26)	8 domande
• **CAPO V:** Gestione dei rischi informatici derivanti da terzi	(artt. 28-30)	8 domande

CAPO II Gestione dei rischi informatici – art.5 Governance e organizzazione
L'organo di controllo....

Domanda	SI	In Parte	NO
ha assunto la responsabilità finale per la gestione dei rischi informatici?			
ha definito chiaramente ruoli e responsabilità per tutte le funzioni connesse alle TIC e stabilito adeguati meccanismi di governance al fine di garantire una comunicazione, una cooperazione e un coordinamento efficaci e tempestivi tra tali funzioni, compreso il ruolo di un responsabile della sorveglianza sull'esposizione al rischio per l'utilizzo di fornitori di TIC?			
ha definito è approvato la strategia di resilienza operativa digitale compresa la determinazione del livello appropriato di tolleranza per i rischi informatici ?			
approva, supervisiona e riesamina periodicamente l'attuazione della politica di continuità operativa delle TIC e dei piani di risposta e ripristino relativi alle TIC ?			
approva e riesamina periodicamente i piani interni di audit in materia di TIC ?			
assegna e riesamina periodicamente le risorse finanziarie adeguate per soddisfare le esigenze di resilienza operativa digitale rispetto a tutti i tipi di risorse, compresi i pertinenti programmi di sensibilizzazione sulla sicurezza delle TIC e le attività di formazione sulla resilienza operativa digitale nonché le competenze in materia di TIC per tutto il personale ?			
approva e riesamina periodicamente la politica dell'entità finanziaria relativa alle modalità per l'uso dei servizi TIC prestati dal fornitore terzo, comprensiva degli aspetti di comunicazione rilevanti ?			

WORK IN PROGRESS

- Indagine di alto livello per auto valutazione realizzato:
  - sulle aree di diretta applicazione per le banche
  - con domande chiuse (Si / In parte/ No)
- Non è uno strumento di validazione
- Si concentra sugli aspetti operativi

DORA è trasversale su molti processi aziendali e riguarda ambiti tecnici, organizzativi, di governance

AMBITO	OBIETTIVI	Governance	Business functions (Operations)	Compliance	Audit	Business Continuity	Risk Management	Data Protection	Information Technology (& Disater Recovery)	Information Security	Procurement	Communication	Human Resources	Facility and Energy Management	Insurance
Capo II – Gestione dei rischi informatici	Quadro per la gestione dei rischi informatici applicabile a tutte le istituzioni finanziarie	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Capo III – Gestione, […] degli incidenti informatici	Nome uniformi per la gestione, classificazione e segnalazione degli incidenti informatici	X	X	X	X	X	X	X	X	X		X			
Capo VI – Test di resilienza operativa digitale	Articolazione dei piani Test di cybersicurezza di base e avanzati (inclusi red teaming)	X	X	X	X	X	X		X	X	X		X	X	
Capo V – Gestione dei rischi informatici derivanti da terzi	Principi per la gestione del rischio di terze parti, Disposizioni contrattuali Quadro di supervisione per fornitori critici	X	X	X	X	X	X	X	X	X	X			X	X
Capo VI – Meccanismi di condivisione delle informazioni	Scambio volontario di informazioni e intelligence sulle minacce informatiche	X					X	X	X	X					

WORK IN PROGRESS

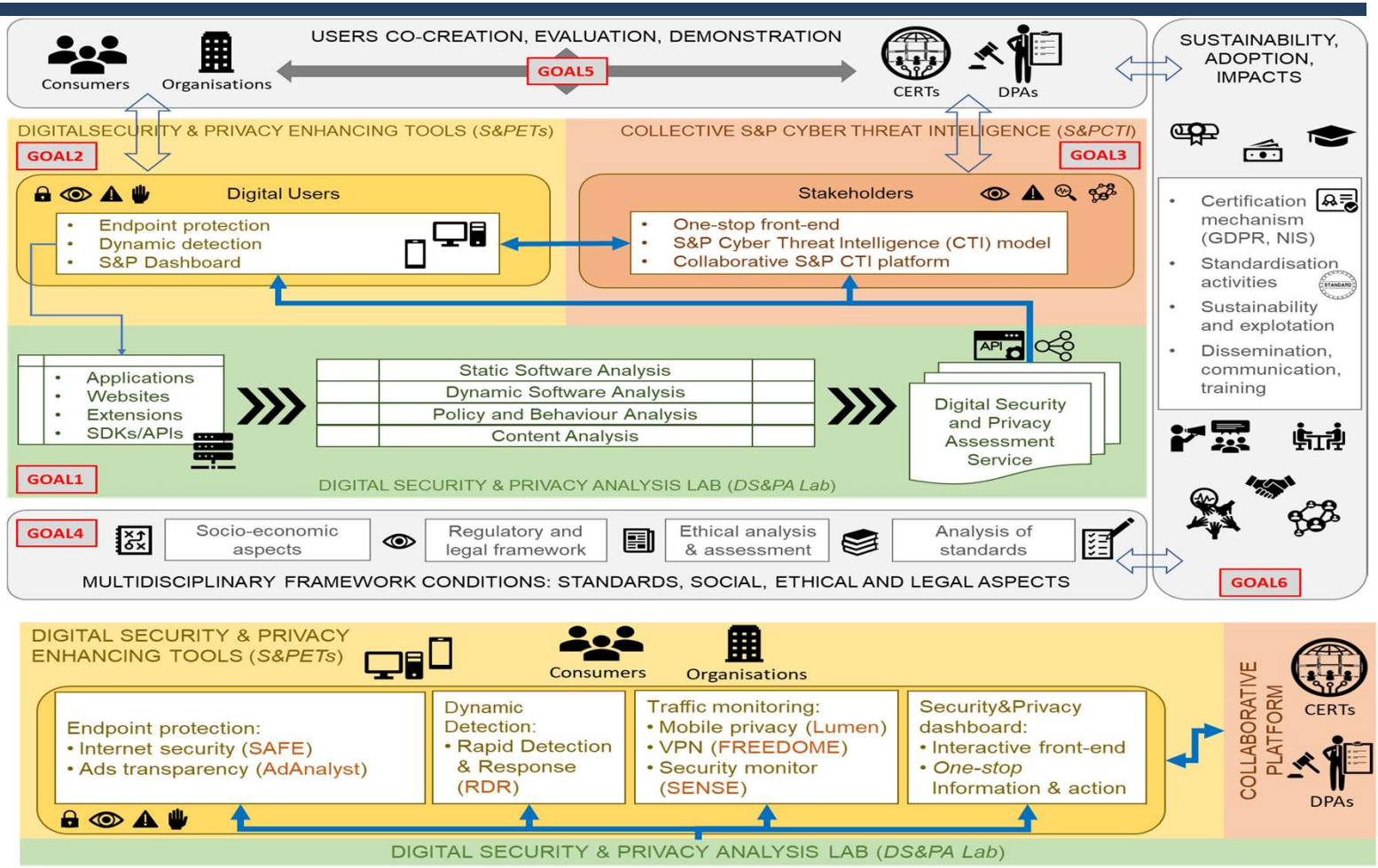
Necessario un **approccio multidisciplinare** per la compliance a DORA

Il punto di vista del **servizio** è un valore per l'azienda per meglio presidiare i rischi digitali in tutta la catena produttiva

La **resilienza come «modo di lavorare** (oltre il costo o obbligo normativo) entra nella cultura di tutta l'azienda e diviene **caratteristica dell'organizzazione**

Proattività di tutte le funzioni aziendali per **rilevare** e gestire **nuovi rischi** e per individuare **opportunità di prevenzione o mitigazione**

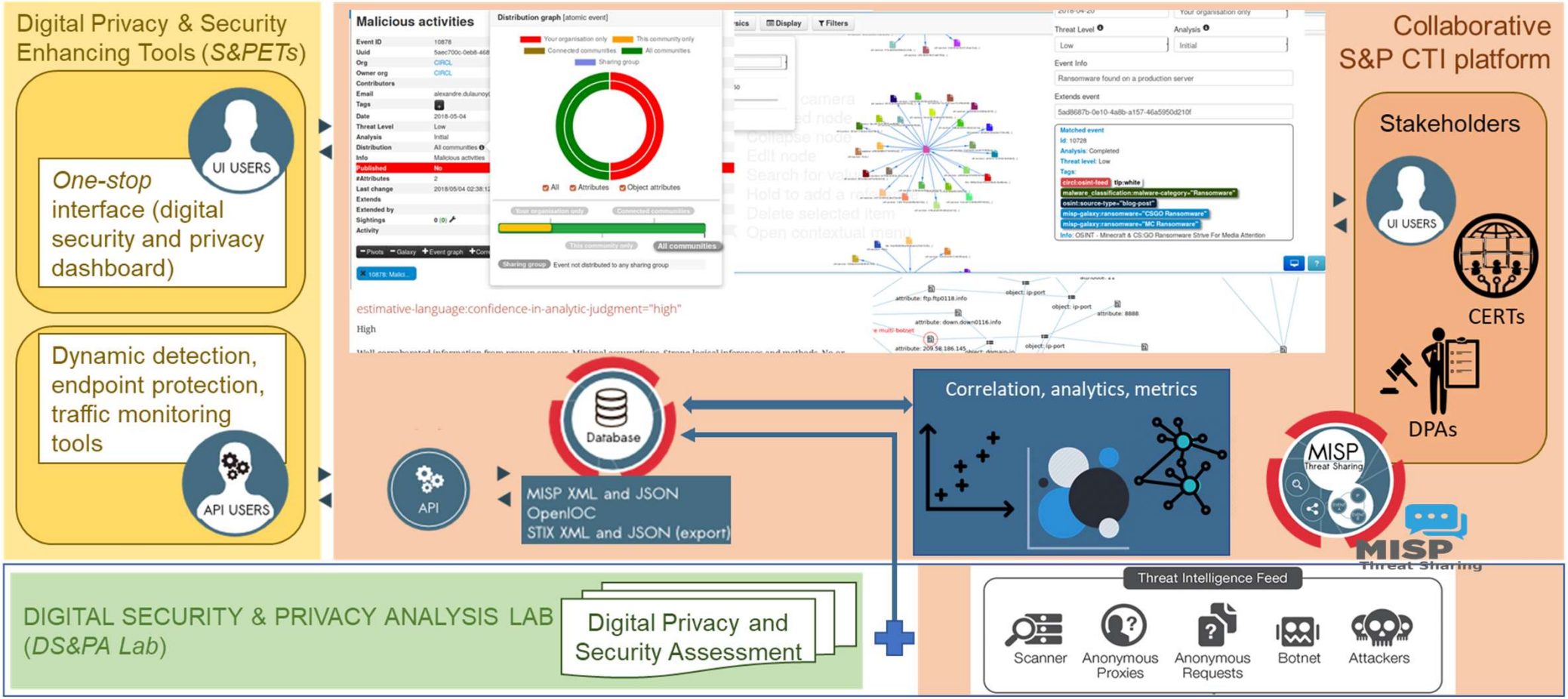
A **holistic digital S&P framework** comprising a set of novel and integrated **tools and services** co-created by citizens and stakeholders (**CERTs**, DPAs, organisations, developers and policy-makers) to **identify, audit, analyse, prevent, and mitigate the impact of the various S&P threats** associated with citizen's digital activities



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

TRUST aWARE

*Providing a **MISP Based collaborative platform** to create and support a S&P-Threat Intelligence environment for citizens, stakeholders, Data Protection Authorities (DPAs) CERTs and other organizations*



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

ricerca@certfin.it
ricerca@abilab.it