UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unIMC

Gestione delle terze parti ICT nel quadro del D.O.R.A

Alessandra Santoro

- Dipartimento di Ingegneria dell'Informazione
- E-mail: alessandrasantoro127@gmail.com
- Telefono: +39 3447476469

Venerdì 3 Ottobre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Introduzione D.O.R.A

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Il D.O.R.A: «Digital Operational Resilience » Act

- La Digital Operational Resilience Act (D.O.R.A) è il nuovo modello europeo per un'efficace ed inclusiva gestione dei temi Cybersecurity ed ICT nei Financial Services, secondo una visione olistica basata sull'integrazione dei rischi e il presidio delle terze parti.
- Si applica a compagnie di assicurazione e riassicurazione, intermediari assicurativi, istituti di investimento, società di gestione, banche, fornitori di servizi di cripto-asset, enti per fondi pensione aziendali e fornitori terzi di servizi ICT.

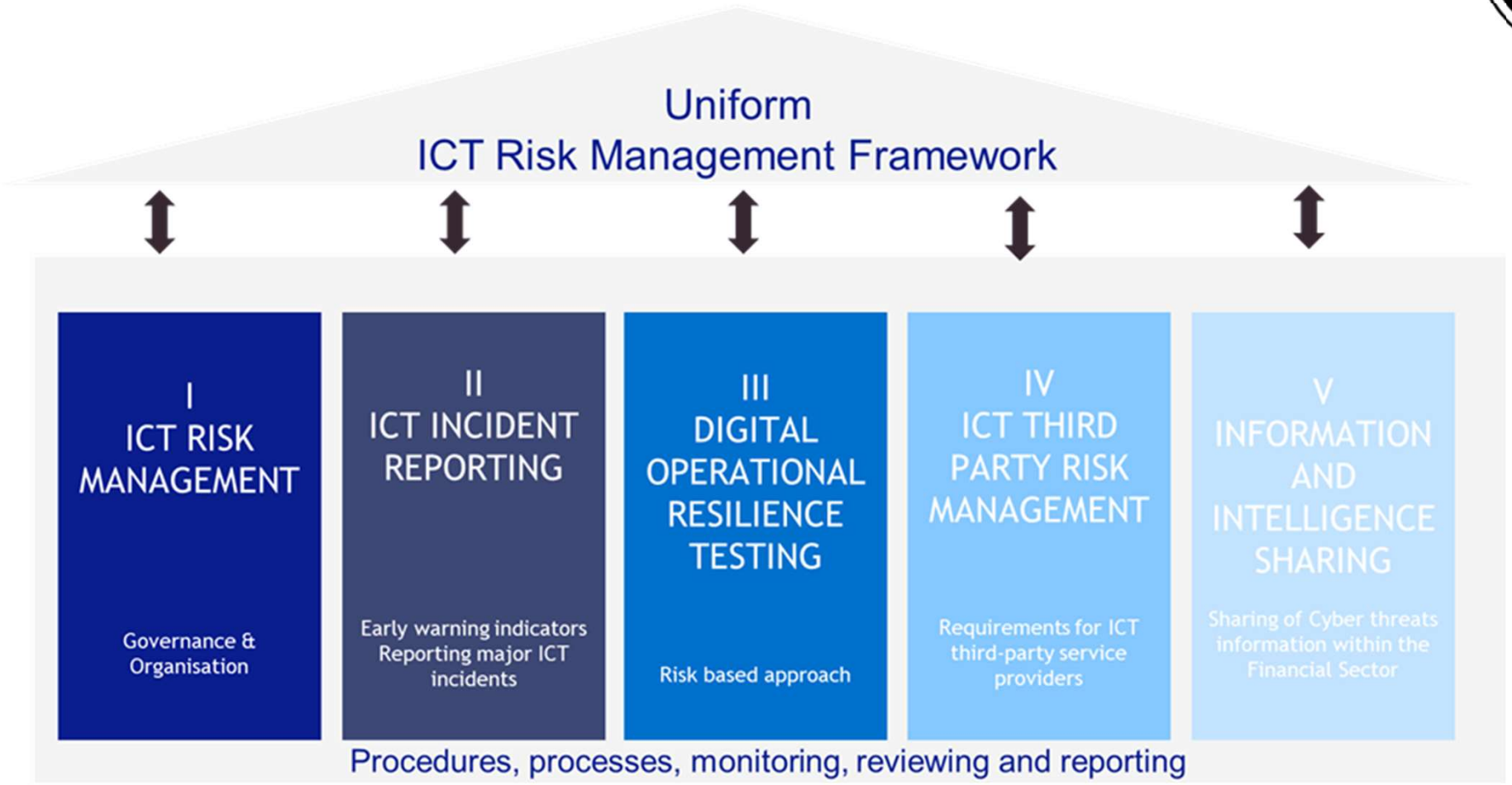
Obiettivo D.O.R.A

- L'introduzione di D.O.R.A mira a ridurre i rischi sociali ed economici dei crescenti cyber-threats nel settore finanziario. Molteplici le cause dell'aumento dei cyber-threats, come l'aumento della connettività della tecnologia informatica tra le organizzazioni, l'esternalizzazione dell'IT a terzi, compresi i fornitori di servizi cloud, la continua digitalizzazione del settore finanziario, compresa la digitalizzazione dei servizi finanziari e delle applicazioni fintech da un lato, e l'esistenza di sistemi legacy vulnerabili all'interno del settore dall'altro.

Pilastri D.O.R.A 1/2

- La legislazione D.O.R.A poggia su cinque pilastri, ciascuno con un focus specifico. L'illustrazione (si veda slide n.7) rappresenta i diversi pilastri. I requisiti specifici di D.O.R.A possono far parte di un quadro uniforme di gestione del rischio ICT per gestire la resilienza digitale di un'organizzazione in modo permanente.

Pilastri D.O.R.A 2/2



ICT Third Party Risk Management

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Contesto normativo D.O.R.A Terze Parti

- Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (Capo V – Gestione dei rischi informatici derivanti da terzi);
- Regolamento delegato (UE) 2024/1774 della Commissione del 13 marzo 2024;
- Regolamento di esecuzione (UE) 2024/2956 della Commissione del 29 novembre 2024;
- Regolamento delegato (UE) 2025/532 della Commissione del 24 marzo 2025.

ICT Third Party Management: requisiti chiave

- Registro delle informazioni (ROI)
- Valutazione e due diligence
- Obblighi contrattuali art. 28-30 2022/2554
- Resilienza e test congiunti
- Incident reporting

Registro delle informazioni (ROI) 1/2

- Il ROI è un inventario dettagliato e dinamico che censisce tutte le relazioni contrattuali con i fornitori di servizi ICT, comprese quelle intra-gruppo.
- In Italia, le entità finanziarie hanno dovuto trasmettere il ROI a Banca d'Italia e/o alle altre Autorità competenti (es. Consob), in formato compresso (pacchetto .zip), entro il 30 aprile scorso.
- https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=OJ:L_202402956

Documento
Adobe Acrobat

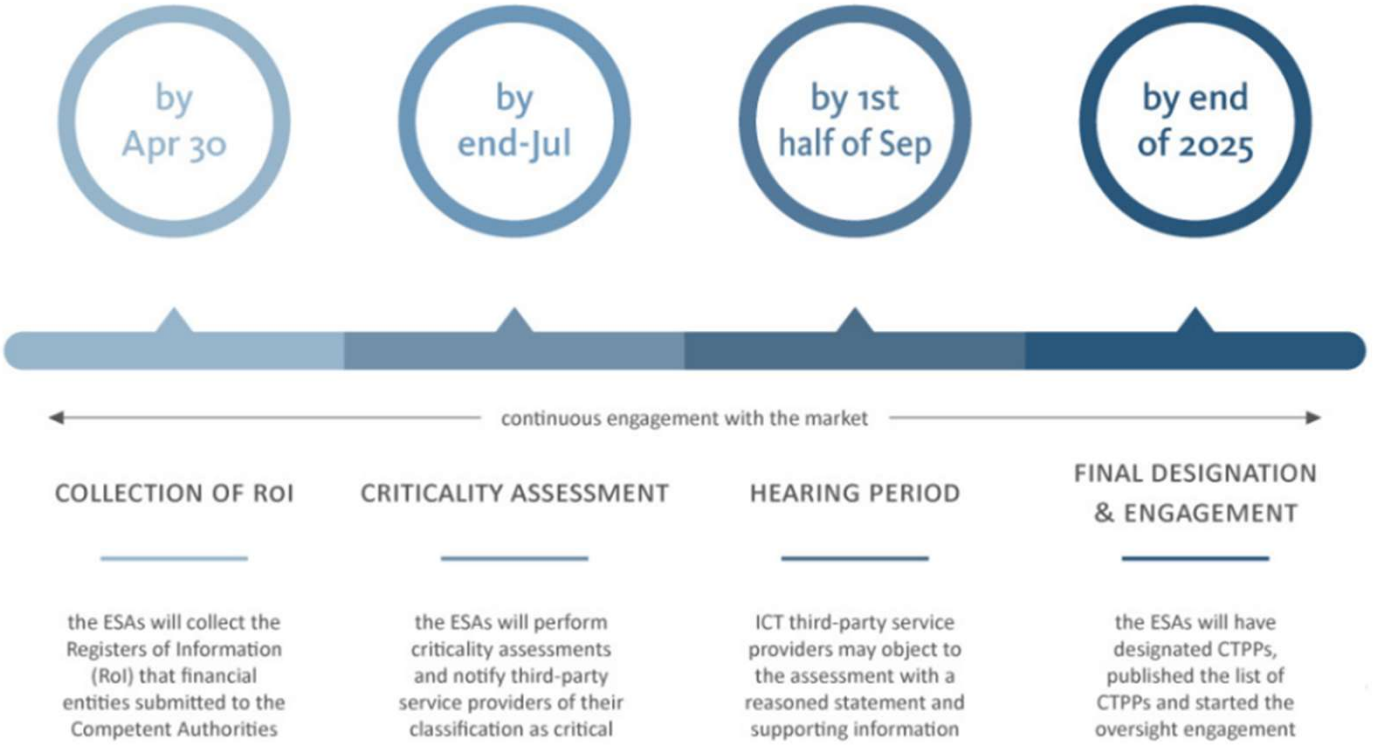
Registro delle informazioni (ROI) 2/2

- Per quanto riguarda la trasmissione del ROI, non è stato ancora definito il termine per il prossimo invio dei dati. Il Registro deve essere mantenuto e aggiornato di continuo e inviato su richiesta dell'Autorità competente.
- Sebbene la legge non preveda termini per la trasmissione del ROI, è ragionevole ipotizzare una cadenza annuale, considerando che Banca d'Italia deve a sua volta trasmettere i dati all'EBA con questa periodicità.
- https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2025_7309

Supervisione dei Fornitori ICT Critici

- Uno degli elementi innovativi introdotti dal D.O.R.A è il meccanismo di supervisione a livello UE dei fornitori ICT terzi «critici». D.O.R.A prevede che alcuni fornitori tecnologici di rilievo sistemico siano designati come «Critical Third-Party Providers» (CTPP) e sottoposti a sorveglianza diretta da parte delle Autorità europee (le ESAs: EBA, EIOPA, ESMA).

Roadmap to the designation of CTPPs by the ESAs



Valutazione e Due Diligence

Valutazione iniziale (Due Diligence)

Analisi preventiva prima di avviare o rinnovare contratti ICT

Verifica standard di sicurezza e resilienza del fornitore

Obbligo art. 28 D.O.R.A: contratti solo con provider conformi

Obblighi contrattuali (art 28-30 2022/2554)

Rinegoziazione e nuovi contratti: adeguamento degli accordi ICT esistenti e predisposizione di contratti conformi per future collaborazioni.

Descrizione dei servizi: chiara e completa per tutti i servizi forniti.

Subappalto: regolamentazione e obbligo di comunicazione dei sub-fornitori critici.

Ubicazione e trattamento dati: data center, giurisdizioni e flussi dei dati chiaramente definiti.

Protezione dei dati: riservatezza, integrità, disponibilità e autenticità dei dati.

Continuità operativa: piani di emergenza e disaster recovery testati.

Audit e accesso: diritto della banca di ispezionare i sistemi del fornitore e partecipazione a audit da parte delle autorità.

Sicurezza ICT: rispetto di standard elevati e gestione delle vulnerabilità.

Segnalazione incidenti: notifica tempestiva degli incidenti ICT (es. entro 4 ore).

Exit strategy: clausole per cessazione ordinata, migrazione dati e continuità operativa.

Controllo su sub-fornitori: visibilità e gestione della catena completa di fornitura (fourth parties).

Resilienza e test congiunti

Coinvolgimento dei fornitori ICT: partecipazione attiva ai programmi di resilienza e training su minacce cyber (Art. 13 DORA).

Test di resilienza congiunti: TLPT ogni 3 anni per le entità più grandi, inclusi fornitori critici.

Cooperazione durante i test: definizione di accordi per garantire sicurezza e riservatezza senza impatti operativi.

Obiettivo: verificare la capacità complessiva dell'ecosistema banca + fornitori di prevenire e resistere ad attacchi sofisticati.

Approccio integrato: elevare la postura di sicurezza di tutti i soggetti terzi coinvolti nelle funzioni critiche.

Incident Reporting

- D.O.R.A introduce un regime armonizzato per la segnalazione degli incidenti ICT gravi alle autorità competenti, come Banca d'Italia, con tempistiche precise: la prima notifica deve essere inviata entro 4 ore dalla rilevazione, seguita da un report dettagliato entro 72 ore e un rapporto finale entro un mese. Questo obbligo si applica anche agli incidenti originati da fornitori esterni, attraverso canali di comunicazione rapidi e clausole contrattuali vincolanti per la notifica immediata.

Conclusioni

- Il Regolamento D.O.R.A segna un punto di svolta nella gestione dei fornitori ICT nel settore finanziario.
- Introduce un quadro normativo chiaro e vincolante, accompagnato da un approccio operativo volto a rafforzare i processi interni e la resilienza complessiva.
- La vera sfida sarà coniugare compliance e innovazione, trasformando gli obblighi regolamentari in prassi aziendali consolidate senza rallentare l'evoluzione digitale.
- Le istituzioni che sapranno integrare il rischio ICT e dei fornitori nelle decisioni strategiche otterranno un vantaggio competitivo, traducendo l'adeguamento normativo in opportunità di crescita sostenibile e affidabile.