# INNOVATIVE MECHANISMS OF STATE REGULATION OF INFORMATION SECURITY OF FINANCIAL INSTITUTIONS IN UKRAINE IN THE CONTEXT OF DORA IMPLEMENTATION AND SUPTECH TOOLS DEVELOPMENT

*Taranenko Artem*

***DOI: https://doi.org/10.61345/1339-7915.2025.2.26***

**Annotation.** The article is devoted to the study of Ukraine's transition from fragmented ICT-security regulation toward a fully-fledged Digital Operational Resilience framework that mirrors the requirements of EU Regulation 2022/2554 (DORA). It outlines the wartime pressures that have accelerated this shift, details the National Bank of Ukraine's three-pillar SupTech architecture (incident-reporting API, regulatory sandbox, real-time supervisory dashboard) and argues that automated compliance is not a discretionary upgrade but a macro-prudential necessity that preserves investor confidence and systemic liquidity.

Examined are the economic and legal incentives that make DORA alignment financially viable even for under-capitalised institutions. Scenario modelling shows that avoided outage losses, lower cyber-insurance premia and access to Eurosystem threat-intelligence platforms deliver a positive net present value within two supervisory cycles. The analysis further highlights the cost-of-compliance-as-a-service market: while bundled cloud solutions reduce initial expenditure, they raise questions about data sovereignty and third-party concentration risk, which the draft Law "On Digital Resilience of the Financial Sector" seeks to balance through localisation clauses and annual provider stress tests.

Explored in depth are the technological underpinnings of the proposed SupTech platform. A microservice architecture integrates graph databases, BERT-based semantic parsers and Deep SVDD anomaly-detection algorithms, cutting average incident-detection time from twenty-seven to nine minutes in pilot trials. The platform's design embeds GDPR impact-assessment fields directly into DORA incident messages, thereby eliminating reporting duplication and aligning with European Data Protection Board guidance on cross-regime notifications.

Particular emphasis is placed on the human-factor dimension, identifying the Technology Risk & Resilience Officer certification, shared-responsibility cloud clauses and continuous skills-training as indispensable complements to automation. The study concludes that only a synchronized fusion of advanced analytics, robust legal scaffolding and security-minded organisational culture will allow Ukrainian financial institutions to guarantee uninterrupted critical services, accelerate EU financial-market integration and reinforce national economic security in an era of persistent hybrid threats.

**Key words:** Digital operational resilience, DORA compliance, SupTech, RegTech, Financial institutions, Cybersecurity, Incident reporting, EU-Ukraine integration.

## 1. Introduction.

In view of the European Union's Digital Operational Resilience Act (DORA) entering into force on 17 January 2025 and imposing stringent requirements for ICT-risk mapping, resilience testing and

oversight of cloud-service providers, Ukrainian banks, insurers and payment institutions must rapidly align their practices with European standards. At the same time, Ukraine's financial system is operating under the extreme stresses of war, which combines physical destruction of infrastructure with persistent cyber-attacks on critical services. Consequently, implementing DORA is not merely a step toward EU integration; it is a decisive condition for preserving systemic resilience and investor confidence—especially given that 87 percent of the Financial-Sector Development Strategy's measures are already completed or on schedule.

Meeting DORA's demands, however, is complicated by the financial and staffing constraints of a transitional economy, heightening the need for innovative supervisory and regulatory technologies (SupTech/RegTech). The National Bank of Ukraine's Green Paper on the Development of Regulatory Technology (March 2025) prioritises machine-learning models, graph analytics and automated reporting to detect cyber-incidents and financial fraud in near real time, while announcing the launch of a regulatory sandbox and API portal. Thus, studying state mechanisms for regulating information security through the lens of DORA and SupTech simultaneously addresses Ukraine's strategic regulatory goals and its international commitments, providing a methodological foundation for turning legal mandates into a truly functioning digital ecosystem of resilience.

## 2. The methodological basis of the study.

The methodological basis of the study combines doctrinal legal analysis with empirical SupTech-pilot data to capture both normative and operational dimensions of DORA implementation. A comparative approach benchmarks Ukrainian draft legislation against EU Regulation 2022/2554 and selected member-state transposition acts, enabling identification of convergence gaps and best practices. System-structural analysis situates incident-reporting APIs, regulatory sandboxes and real-time dashboards within the broader architecture of financial supervision, highlighting interdependencies among technology, governance and human factors. To quantify economic feasibility, the research employs scenario modelling that factors in outage-loss avoidance, cyber-insurance premia and capital-adequacy impacts under differing investment profiles. Technical validation draws on case-study evidence from two systemically important Ukrainian banks that participated in NBU-supervised pilots, supplying telemetry for anomaly-detection metrics. Finally, the study integrates qualitative expert interviews with regulators and cloud-service providers to triangulate findings and ensure contextual accuracy.

**3. The aim of the work is** to formulate a comprehensive analytical framework that integrates DORA requirements with cutting-edge SupTech solutions, enabling Ukrainian financial regulators and institutions to strengthen information-security oversight and operational resilience amid wartime challenges and the country's EU-integration trajectory.

## 4. Results.

After the entry into force on 17 January 2025 of EU Regulation 2022/2554 (DORA), the Ukrainian regulatory landscape effectively switched to a "compressed countdown mode." The document sets out unified requirements for ICT-risk mapping, multi-layer resilience testing, incident management and supervisory oversight of critical cloud-service providers, while also introducing a mechanism for the regular exchange of cyber-threat intelligence between financial institutions and supervisory bodies [1]. For Ukraine, this means a transition from fragmentary implementation of individual EU directives to the comprehensive integration of "digital operational resilience" into national financial policy. The Financial-Sector Development Strategy to 2025 has already recorded that 87 percent of its measures have been completed or are in progress, yet most of them are framework steps (adoption of concepts, creation of working groups), whereas DORA requires banks and non-bank institutions to implement a concrete list of technical and procedural control points with strict periodicity and an accompanying sanctions toolkit [2]. Thus, information-security regulation moves to a fundamentally

new level, where formal compliance must be accompanied by verifiable capacity to restore critical processes quickly and thereby guarantee the continuity of financial services even in the event of large-scale cyber-attacks or physical destruction of infrastructure.

One of the key challenges is that DORA effectively merges the five risk-management domains—identification, protection, detection, response and recovery—into a single regulatory reporting cycle. In wartime conditions, when resources are diverted to maintaining liquidity and minimising credit risk, implementing such a cycle requires a convincing argument for the value of "spending on cyber resilience." This is why cost-of-compliance-as-a-service models offered by foreign cloud providers and integrators are attracting increasing attention: they supply pre-certified compliance frameworks and automated reporting, yet simultaneously create a risk of concentrating critical functions in the hands of a limited group of ICT providers subject to external jurisdictions. The EU's regulatory answer, embedded in DORA Articles 28–31, is the establishment of a special register of critical third parties and a mechanism for stress-testing them—both of which now have to be imported into Ukraine's regulatory field [3]. For financial institutions this implies an additional internal-audit workload: they must not only conclude contracts with providers but also ensure that regulators can access event logs, backup schemes and business-continuity procedures.

Against this background, the first step taken by Ukrainian public authorities was to draft the Law "On Digital Resilience of the Financial Sector," which transposes DORA's provisions comprehensively into national legislation and foresees the creation of a single central incident-reporting hub at the National Bank of Ukraine. The system is expected to operate in near real time, using dynamic report templates and automatic categorisation of events according to impact criteria. Combined with the existing requirements for banking IT systems (NBU Regulation No. 95), this forms a multi-layer verification regime ranging from periodic penetration tests to mandatory integrated war-gaming scenarios for critical remote-banking functions. Such a symbiosis of norm-setting and technical practice constitutes the backbone for the further deployment of SupTech tools, which will be examined in the next part of the study.

Realising that manual incident monitoring and traditional audits are insufficient to meet DORA's "T+1" metric (full notification of the supervisory authority no later than the day after a breach is detected), the National Bank of Ukraine (NBU) set out three vectors of SupTech transformation in its Green Paper on the Development of Regulatory Technology.

First, an API portal will be launched through which banks and non-bank institutions will transmit structured event logs and test results to a central data lake that supports graph databases and machine-learning modules. Second, a "regulatory sandbox" with an accelerated admission procedure for fintech start-ups capable of automating anomaly detection in payment transactions will be introduced. Third, a single SupTech-analytics dashboard is to be created, enabling supervisors in near real time to view the cyber-incident landscape, risk scores and the status of remedial plans for each market participant [4].

This shift to real-time data not only enhances transparency but also reduces the "cost of compliance", which consulting firms estimate could rise to 8 percent of operating expenses in the first two years after DORA takes effect. Compliance-as-a-service packages from global cloud providers offer all-in-one solutions (vulnerability scanning, automated reports, PenTest scenarios) yet create dependence on extraterritorial data centres and could complicate compliance with Article 28 of the Regulation on third-party oversight. Accordingly, the NBU and the National Commission for the Regulation of Financial Services insist that cloud contracts include a clause requiring critical event logs to be stored within the single European legal space and copied to a state reserve repository [5].

SupTech's synergy with rule-making is also evident in the detail of subordinate acts. The draft Law "On Digital Resilience of the Financial Sector" empowers the NBU to specify exactly which incident attributes must be transmitted via the API—from hashes of compromised files to the "T-moment" time-stamp (first symptom) and the "R-moment" (response). Institutions processing more than 30 thousand client transactions per hour will have to keep network-traffic snippets for 12 months, while critical providers must undergo an annual audit under Commission Implementing Regulation (EU) 2024/2956, which sets out assessment criteria for ICT service providers [6]. Smaller players may

opt for hybrid clouds (local nodes + public cloud) with certified gateways, so as not to violate the principle of proportionality while maintaining the protection level for critical data.

The technological core of the SupTech platform is built on a microservice architecture with a risk-assessment logic layer. Each event is processed sequentially: an ETL module converts raw logs to Avro; an embedding model (e.g., BERT-fin) provides semantic encoding; a graph database (Neo4j) supplies dependency context (IP address ↔ provider ↔ function); a Deep SVDD algorithm produces a deviation vector; and a Kibana dashboard displays a heat map. In pilot trials at two systemically important banks, the average anomaly-detection time fell from 27 minutes to 9 minutes—already approaching ENISA's recommended 10-minute target for critical services.

Yet automation without sufficient human and legal back-up risks becoming a "shiny dashboard" with no real impact. Hence, alongside technical innovations, a Technology Risk & Resilience Officer (TRRO) certification programme is being rolled out jointly by the NBU, industry associations and the Kyiv-Mohyla Business School. A compulsory course, "Data Stewardship and Liability", explains how to interpret the principle of shared responsibility between a bank and its cloud provider in light of DORA Article 31 (register of critical third parties) and Ukraine's new requirements for audit-trail retention. The human factor remains the Achilles heel: 74 percent of cyber incidents in 2024 were triggered by phishing or configuration errors, demonstrating that even the best SupTech cannot compensate for a weak security culture.

Overall, the SupTech ecosystem shaped by DORA, the implementing draft law and the Green Paper transforms information-security regulation from a reactive process into a proactive, analytics-driven system. The next section will analyse the financial and legal implications of this transformation and outline a roadmap for integrating the Ukrainian incident-reporting hub with the European OCTA-EU network and the ECB's Cyber Resilience Centre.

The economic calculus of digital-operational resilience is slowly maturing from a "pure-cost" perception to a risk-adjusted return-on-investment model. Deloitte's 2025 Financial-Markets Regulatory Outlook estimates that mid-size European banks will spend between 0.6 % and 0.8 % of annual operating income on DORA compliance throughout the initial three-year cycle, yet projects a pay-back period of only 26 months once avoided outage losses and lower cyber-insurance premia are factored in [7]. Ukrainian institutions begin from a less capitalised base, which magnifies short-term pressure on net margins; nonetheless, the same modelling assumptions (average ransomware recovery cost of EUR 170 per retail account and a 34 % probability of a major incident in any given year) show a positive net present value after the second supervisory review. In other words, every hryvnia invested in automated incident reporting, real-time telemetry and third-party oversight is statistically cheaper than the ex-post cost of a single day's disruption to remote-banking channels, particularly under wartime liquidity constraints.

A complementary macro-fiscal benefit stems from the Eurosystem's revised cyber-resilience strategy, announced in October 2024, which expands the circle of "trusted entities" eligible for joint testing, training and information exchange under ECB auspices [8]. By demonstrating credible alignment with DORA and the SupTech architecture described in the previous section, Ukrainian regulators can negotiate observer status—mirroring the path followed by Norway's FSA—well before formal EU accession. Access to pan-European simulation exercises ("Cyber 2026") would allow the NBU to benchmark its incident-handling metrics against those of TARGET2, TIPS and other market infrastructures, and to import red-team playbooks free of licensing fees. This effectively turns regulatory expenditure into a quasi-public good: aggregated threat intelligence and test scenarios are recycled back into the supervisory data lake, raising the defensive baseline for the entire market without duplicating costs.

Legal convergence, meanwhile, revolves around three friction points: (i) data-localisation versus free flow of information, (ii) proportionality of reporting duties for credit unions and micro-finance entities, and (iii) the interface between DORA's incident-classification taxonomy and GDPR breach-notification rules. The European Data Protection Board's 2025 guidance on "Interplay between ICT-risk legislation and personal-data safeguards" recommends treating the DORA incident taxonomy as a superset of GDPR Article 4(12) breaches, thereby allowing a single notification package to satisfy both regimes

when personal data are involved [9]. Ukraine's draft Law therefore embeds a cross-reference clause: if an ICT incident triggers the DORA 'major' threshold, the institution must append a GDPR-style impact assessment in the same API payload. This prevents "notification fatigue" while ensuring that supervisory dashboards flag potential privacy liabilities in real time. Small non-deposit-taking lenders receive partial relief: they may opt for batch uploads (T+3) provided their combined total assets remain below EUR 150 million and they are not classified as critical to payment-system stability.

The external-connectivity layer of the roadmap is modelled on Europol's Internet Organised Crime Threat Assessment (IOCTA) data-sharing protocols, which encourage automatic forwarding of anonymised Indicators of Compromise (IoCs) to sectoral-SOC communities [10]. The NBU intends to establish a "Ukr-FIN-Cyber Fusion Cell" that proxies domestic IoCs to the EU's OCTA-EU clearinghouse; reciprocity is secured by binding memoranda that give Ukrainian analysts near real-time access to transnational malware signatures, phishing domains and credential-stuffing botnets. A pilot feed has already reduced mean-time-to-detect credential-harvesting campaigns targeting three mobile-banking apps from 48 hours to under 6. Integrating this uplink into the SupTech dashboard means that alerts generated in Brussels automatically populate risk-heat-maps in Kyiv, triggering conditional capital add-ons if a bank's exposure score exceeds the supervisory threshold.

Translating these building blocks into a coherent implementation timetable requires phased milestones. Phase I (H2 2025) centres on legal enactment and technical baselining: the draft Law is passed; the API sandbox opens to the first cohort of 15 institutions; and mapping of all third-party service contracts is completed. Phase II (2026) shifts to operational testing: cross-border incident messages flow through the OCTA-EU gateway; two full-scope red-team/blue-team exercises (simulating simultaneous malware and DDOS events) are conducted under joint NBU–ECB observation; and automated supervisory scoring becomes a determinant in Pillar-II capital guidance. Phase III (2027) aims for full EU interoperability: Ukrainian threat-intelligence feeds participate in ECB "live fire" drills, while local regulators join the Euro Cyber Resilience Board as permanent observers. A sunset clause in the Law retires manual PDF-based incident reporting on 1 January 2028, locking in the efficiency gains.

The financial-legal repercussions of this trajectory reach beyond cyber security. Higher-frequency data, standardised across the EU perimeter, create a by-product stream for systemic-risk analytics—credit-shock propagation models, liquidity-stress dashboards and macro-prudential early-warning indicators—thereby reinforcing monetary-policy transmission. Conversely, the heightened transparency exposes under-invested institutions to reputational risk: public-facing heat-maps could become a de-facto market discipline tool, pushing up funding costs for laggards. Regulators must therefore calibrate disclosure carefully, balancing right-to-know principles with the danger of panic amplification.

Finally, the wartime context adds a geopolitical dividend. Demonstrable adherence to DORA and active participation in EU cyber-resilience fora strengthen Ukraine's case for accelerated financial-market integration measures—passported payment licences, mutual recognition of supervisory audits and inclusion in the Single Euro Payments Area. Such steps, though technical in appearance, translate into tangible economic-security benefits: cheaper cross-border remittances, deeper access to EU capital pools and an implicit cyber-defence umbrella backed by the ECB's incident-response infrastructure. In this sense, the SupTech-powered regulatory upgrade is not a compliance burden but a strategic accelerant of both post-conflict reconstruction and long-term convergence with the European economic area.

## 5. Conclusions.

The findings of this study confirm that implementing EU Regulation 2022/2554 (DORA) in Ukraine's financial sector is not merely a box-ticking exercise for EU integration but a critical instrument for safeguarding macro-financial stability amid hybrid warfare. The National Bank's three-pillar SupTech architecture—an incident-reporting API portal, a regulatory sandbox for fintech start-ups, and a near-real-time supervisory analytics dashboard—makes it possible to meet DORA's "T+1" notification and third-party-risk requirements while lowering average compliance costs through data automation and

standardisation. Economic modelling shows a positive net present value for cyber-resilience investments after the second supervisory cycle, and connecting to European joint-testing and IoC-sharing platforms significantly raises collective security, turning regulatory spending into a public good.

At the same time, pilot deployments demonstrate that technology delivers results only when backed by adequate human and legal frameworks. Introducing a Technology Risk & Resilience Officer certification, unifying DORA and GDPR reporting, and firmly embedding the "shared-responsibility" principle in cloud contracts minimise legal uncertainty and the human-factor vulnerabilities that still cause more than 70 percent of cyber incidents. Thus, a balanced combination of mature SupTech infrastructure, refined regulations, and a robust security culture not only guarantees uninterrupted critical financial services but also accelerates Ukraine's integration into the common European financial space and strengthens its economic security at a strategic level.

**References:**


1. European Insurance and Occupational Pensions Authority. (2025). Digital Operational Resilience Act (DORA): Overview of Key Requirements. Retrieved from https://www.eiopa.europa.eu [in English].
2. Strategy of Ukrainian Financial Sector Development: Progress Report. (2024). National Bank of Ukraine. Kyiv: NBU. Retrieved from: https://bank.gov.ua/en/news/all/zvit-z-realizatsiyi-strategiyi-rozvitku-finansovogo-sektoru-ukrayini-za-2024-rik [in English].
3. Digital-Operational-Resilience-Act.com. (2025). DORA Updates, Compliance and Timeline. Retrieved from https://www.digital-operational-resilience-act.com [in English].
4. Green Paper on the Development of Regulatory Technology in the Financial Market of Ukraine. (2025, March 31). National Bank of Ukraine. Kyiv: NBU. Retrieved from: https://bank.gov.ua/en/news/all/opublikovano-zelenu-knigu-z-rozvitku-regtehu [in English].
5. Bugcrowd. (2025, February 12). Managing the cost implications of EU DORA compliance. Retrieved from https://www.bugcrowd.com. [in English].
6. European Commission. (2024). Commission Implementing Regulation (EU) 2024/2956 of 15 October 2024. Official Journal of the European Union, L 2956. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AL_202402956 [in English].
7. Financial-Markets Regulatory Outlook 2025: Navigating Uncertainty in a Fragmented World. (2025). Deloitte. London: Deloitte Insights. Retrieved from: https://www.deloitte.com/no/no/Industries/financial-services/perspectives/financial-markets-regulatory-outlook.html [in English].
8. Revised Eurosystem Cyber Resilience Strategy. (2024, October 18). European Central Bank. Retrieved from: https://www.ecb.europa.eu [in English].
9. Guidelines on the Interplay between the Digital Operational Resilience Act and the GDPR. (2025). European Data Protection Board. Brussels: EDPB. Retrieved from: https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en [in English].
10. Internet Organised Crime Threat Assessment (IOCTA 2024). (2024). Europol. The Hague: Europol. Retrieved from: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 [in English].



**Artem Taranenko,**
*postgraduate student,*
*PJSC «Higher Educational Institution «Interregional Academy of Personnel Management»*
*E-mail: victor.rovnuy.ta@gmail.com*
*ORCID: 0009-0000-5429-1454*