Sheltered Harbor Position on Support for DORA

E.U. Digital Operations Resilience Act

Sheltered Harbor LLC
October 2025

Position on Support for DORA

October 2025

TABLE OF CONTENTS

Position on Support for DORA

October 2025

Executive Summary

The Digital Operational Resilience Act (DORA) is a comprehensive set of regulations that apply to financial entities that operate in the European Union. It is aimed at enhancing the digital resilience of financial entities. Sheltered Harbor is a financial sector framework that covers data vaulting standards and guidance to prepare a financial institution to survive a severe operational outage. Sheltered Harbor, a private not-for-profit entity, was established in 2015, with support from American regulators for the purpose of maintaining public confidence in the financial system should a financial institution become operationally disabled, as might occur from a devastating cyber attack[1]. Sheltered Harbor's resilience standards and guidance help financial institutions prepare to survive a severe operational outage and satisfy key regulatory mandates in the process.

DORA advocates for resilience of all Information and Communications Technology (ICT) such that it would protect from, withstand, and recover from significant disruptions. Sheltered Harbor's resilience focus is on the financial institution's preparedness to withstand and recover from a severe disruption. The Sheltered Harbor approach, supported by specifications, tools and, industry-specific guides, is perfectly aligned to start on some of the the more challenging aspects of implementing DORA for the highest risks in today's digital operations.

There are similarities and differences between these two frameworks. For example, both advocate for the protection of data, so that it can survive any type of disruption, and both encourage clarity and resilience for the financial entity's Minimum Viable Operation (MVO). Sheltered Harbor's approach is focused on withstanding and prompt resumption

[1] Sheltered Harbor's operations are focused exclusively on establishing, promoting and certifying standards and best practices for the protection of vaulted data and implementation of plans for prompt resumption of critical business services. It holds no operational data for any of its participants and is independent of sovereign entities.

of critical business services after a severe disruption. Whereas DORA's scope is intended to cover all operational ICT requirements, including for disruptions of lesser magnitude. Sheltered Harbor's specifications, tools, and guides are mostly technology agnostic, where some of DORA's standards promote detailed technology compliance.

Sheltered Harbor's position is that financial entities that operate in the EU should consider using the Sheltered Harbor approach to expedite their compliance with one of DORA's most challenging requirements. Sheltered Harbor's objective is consistent with DORA as it relates to enabling a financial institution to withstand and recover from a severe disturbance and, through Sheltered Harbor certifications, to demonstrate compliance with DORA's requirements for this scenario. Sheltered Harbor vaulting standards are globally accepted as the definitive approach to ensure that data is protected from loss of availability, regardless of the cause. Further, Sheltered Harbor's implementation guides lay a groundwork for continuing to assess and address business and technology operational risk and mitigations for less severe outages.

Two Frameworks with Common Intents

Resilience is a broad topic and has been a focus of banking operations forever. Both Sheltered Harbor and DORA exist because the potential impact of some current risks could be devastating to today's digital society. Over the last decade governments around the world have been seeking to mitigate the potential that a devastating outage of digital financial operations could cause the collapse of their economy. In 2015 The U.S. Department of the Treasury hosted a public-private exercise to uncover how the U.S. financial sector would deal with the total operational outage of a financial institution. A result of that exercise was the creation of Sheltered Harbor as an industry initiative with the mission to protect critical data and maintain public confidence in the case of a severe outage that would disrupt a financial institution's operations.

This document will discuss the clear differences in scope between DORA and Shelterered Harbor and identify where implementing Sheltered Harbor's approach for prompt resumption and eventual recovery of critical services supports DORA compliance, and can expedite a financial institution's broader journey toward operational resilience. It will also provide helpful tips for institutions that are seeking to define and address the resilience of their minimum viable operations.

Scope

A clear difference between Sheltered Harbor and DORA is their overall scope. DORA articulates a set of regulations that must be met by a majority of financial entities in the European Union to demonstrate the resilience of their digital operations[2]. It accomplishes this with standards around Information Communications Technology (ICT) and examinations to enforce the adherence to the standards. Sheltered Harbor's focus is narrower – predominantly on the response and resumption of critical data and critical operations after a devastating outage that would prolong recovery to normal operations.

[2] See scope of DORA Article 2 at https://www.digital-operational-resilience-act.com/Article_2.html

Sheltered Harbor, a voluntary framework for financial institutions, relies on independent audits and certifications to prove that its standards have been properly implemented.

Both frameworks focus on resilience, but approach it from different perspectives. Sheltered Harbor assumes that financial entities have mature and sufficient Business Continuity and Disaster Recovery (BC/DR) programs that are capable of recovering full, normal operations – except that they may take longer than necessary for an extreme outage. Sheltered Harbor's approach is to augment existing BC/DR programs by implementing enhanced data protection and an alternative approach for resumpiton of critical services to support the MVO on a temporary restoration platform. This interim platform would be replaced after the BC/DR efforts restore normal operating capabilities. Conversely, EU regulators approached resilience more broadly around critical workloads and advocate for upgrades to the corresponding ICT operations, such that they can withstand any disruption (small or large). Yet, DORA assumes that "Severe ICT-related incidents are not a remote risk, but an inevitable possibility," and advocates that financial entities escalate their ability to withstand and recover, not just protect against the possiblity.

Both frameworks acknowledge that achieving full resilience will take time and require changes to resources. DORA advocates that financial entities should expedite resilience efforts to mitigate highest risks first. Sheltered Harbor, which is focused on risk scenarios with the highest impact, offers a well articulated roadmap and milestones for a program to prepare a financial entity to survive a severe outage. This roadmap is acknowledged by global regulators to be consistent with their intents for resilience, and is supported by mature specifications and guidance for vaulting data and resilience planning.

Defining the path to resilience is one of the earliest challenges for any organization contemplating such a program. Sheltered Harbor provides an excellent starting point; clear guidance on how to make progress; certifications to prove compliance; and an ecosystem of Alliance Partners that can help any financial entity to complete their plans and their journey toward digital operations resilience.

Approach

DORA implementation guidelines advocate that a financial entity should focus their operational resilience efforts first on areas of highest risk. Sheltered Harbor is exclusively focused on the area that the industry consistently proclaims as its highest risk – that is the impact of a cyber issue that causes a devastating operational outage. While Sheltered Harbor's approach to resilience is deeply focused on prevention of a catastrophic data loss and the prompt resumption of critical business services, the standards and tools that the industry developed to address this scenario are highly applicable to issues of lesser magnitude. Implementing the Sheltered Harbor approach addresses the highest risk first and prepares the financial institution to grow that program to address other operational risk as it matures. For example, in defining the characteristics and proof points for a cyber resilient vault, Sheltered Harbor's vaulting standards are useful for protecting the availability of any data, regardless of the purpose for its isolation.

Proof / Compliance

DORA incorporates standards around Information Communications Technology to support resilience of digital operations. The regulation is enforced by the examination of compliance to these standards, and each financial entity is responsible to provide evidence of such. Sheltered Harbor provides certifications, supported by a well-documented adherence framework and independent audits/reviews of the financial institution's implementation of the Sheltered Harbor vaulting processs and resilience plans.

Sheltered Harbor's specifications and guides have been reviewed and are supported by U.S. regulators as proof of the type of resilience that Sheltered Harbor addresses. For example, the Federal Financial Institutions Examination Council (FFIEC) included Sheltered Harbor in its examination handbook as an example of addressing the

resilience of customer account information[3]. In a joint statement about Heightened Cybersecurity Risk, the FDIC and OCC identify Sheltered Harbor as an example of industry best practices and frameworks for resilience[4].

Regulators around the globe value Sheltered Harbor's Certifications for its vaulting standards and resilience planning guides because they incorporate a well defined roadmap and adherence framework, which is the basis for assessments necessary for Sheltered Harbor certifications. Sheltered Harbor provides maps for its underlying control framework against other recognized risk frameworks so that it is easy to align Sheltered Harbor's deliverables with related resilience work.

Sheltered Harbor's certification provides evidence that not only is the architecture compliant, but that the processes for loading and unloading the vault are properly controlled and reliable.

Sheltered Harbor is working with regulators across the globe to ensure alignment of Sheltered Harbor certification requirements to evidence that some important factors of operational resilience are in place[5].

[3] https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/

[4] https://occ.gov/news-issuances/bulletins/2020/bulletin-2020-5a.pdf

[5] Sheltered Harbor's activities with regulators, include coordination with: The Federal Reserve, the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the Securities and Exchange Commision (SEC) and others in the United States; as well as the Monetary Authority of Singapore (MAS); the Prudential Regulatory Authority (PRA) and the Financial Conduct Authority (FCA) in the United Kingdom, the Taiwan Financial Supervisory Commission (FSC), the Hong Kong Monetary Authority (HKMA), the Federal Financial Supervisory Authority (BaFin) of Germany, and others.

Data Protection and Data Vaulting

Data risks are a central part of DORA Information Communications Technology (ICT) risk management, since the regulation treats data as critical assets for the continuity of financial services. DORA rquires financial entities to identify, manage and mitigate data-related risks (availability, integrity, confidentiality, loss, etc.) under its ICT risk management standards.

Financial entities throughout the globe have mature processes to mitigate data-related risks through (a) maintaining comprehansive data backups, recovery and integrity checks; (b) ensuring end-to-end encryption and secure data transmission; (c) performing regular testing of data recovery and integriry checks. While these efforts signifigantly reduce residual data risks, many financial entities have failed to address a catastrophic failure - loss of critical data in both primary and backup systems. Today's risks include severe scenarios (like a dedicated cyber attack) where a prompt failover of critical services to surviving disaster recovery platforms, and recovery of normal operations may not be possible in a short timeframe.

Sheltered Harbor Data Protection and Data Vaulting standards, in the form of specifications and implementation guides, address this gap through the maintainance of isolated tertiary copies of critical data backups which protect them from cyberincidents. The standards cover identification of critical data backups, implementation of the Sheltered Harbor Vaulting Process to store copies of critical data backups in a cyber-resilient, immutable data vault, and provide clarity around controls that are required for data recovery and integrity checks.

To identify critical data, Sheltered Harbor instructs financial institutions to first identify critical services and than map them to supporting data. This is equivalent to ICT and Data Dependency Mapping prescribed by DORA. As a part of critical data identification, financial entities should establish Recovery Time Obejctives (RTOs) and Recovery Point Objectives (RPOs) for related data segments. These RTOs / RPOs define parameters of the vaulting and recovery processes and can be different from ones used for regular backups.

Sheltered Harbor's vaulting standards define requirements for the data vault that ensure data protection: isolation, imutability, confidentiality, security and recoverbility. The standards cover the data vaulting process, which includes malware screening, security, monitoring, and process automation for inserting data into a vault, as well as data recovery requirements for isolation from the production environment and integrity checks.

Sheltered Harbor standards specify multiple control objectives along with illustrative contols that should be met as part of the Vaulting Process implementation. The standards prescribe a formal implementation review and regular (at least annual) data recovery tests with integrity checks.

To assure internal and external stakeholders, including regulators, of adequate protection of critical data, financial institutions can apply for Sheltered Harbor Data Vaulting Certification. This requires an independent review/audit of controls defined in Sheltered Harbor's vaulting specifications.

Sheltered Harbor Alliance Partners offer turnkey solutions that can help financial institutions to implement the Data Protection / Vaulting Process standards.

By incorporating the Sheltered Harbor data protection approach into its BC / DR plans, a financial institution significantly enhances its ability to recover and continue delivery of critical business services.

Maintaining Minimum Viable Operations

Minimum Viable Operations

Operational Resilience is a central objective of DORA. Financial entities have well-developed BC / DR programs. While these efforts signifigantly enhance their ability to withstand and recover from potential discruptions and continue delivering critical business services, few of them address prolonged outages under extreme disruption scenarios. Such scenarios, may also arise from other ICT failures or just from the sheer scale of recovery tasks.

Sheltered Harbor Resilience Planning standards address this gap by focusing on prompt resumption of time-sensitive critical business services on a transitional *Restoration Platform*[6].

To identify time-sensitive critical business services that can support the MVO during a prolonged recovery of normal operation, financial entities are instructed to establish outage tolerances for a full set of critical services and to select ones with tolerances shorter than the maximum expected duration of recovey. You must establish RTOs and RPOs for resumption of critical business services that would rely upon the *Restoration Platform*. The identified time-sensitive services should be mapped to the critical data and ICT systems that support their operations.

Sheltered Harbor standards provide requirements for the *Restoration Platform*:

- Capability to support time-sensitive critical services for the duration of recovery.
- Capability to be deployed and activate services within established RPOs.
- Capability to conduct acceptance testing prior to services activation.
- Isolation from production environment and enhanced risk protection.

Financial institutions should implement the *Restoration Platform* as soon as possible. This could include a combination of existing or new ICT systems, low-risk outsourced services and manual workarounds. An early part of Restoration Platform implementation is identification of system and business data that is necessary to deploy and operate the platform.

[6] Restoration Platform is a concept in Sheltered Harbor's resilience plans that can take many forms. These include a shared 'disaster recovery' platform that can be 'turned on' to support a stricken entity; use of another entity's operating platform; or a self-implemented subset of the stricken entity's technology platform that is isolated from the production environment and can be operational on short notice.

Financial institutions should implement the *Sheltered Harbor Vaulting Process* to protect this data (or confirm that its implemented vaulting process meets Sheltered Harbor requirements).

Preparing to Recover

To ensure the prompt resumption of critical business services in the event of a severe incident, the FEs must develop a comprehensive *Sheltered Harbor Resilience Plan*. This plan must address key decisions, and organizational arrangements, as well as detailed business and technical processes (playbooks, runbooks, screenshots, contracts, etc.), for prompt service resumption.

The Sheltered Harbor standards provide guidelines for the plan development and expect it to include the folowing critical sections:

- Resilience Targets - key decisions made by senior management (targeted critical services and their outage tolerancesand, their RTOs, maximum duration of their operation, etc) and serve as requirements for the rest of the plan sections.
- Incident Management – steps, timeline, decisions, decision-makers and criteria for managing activation and execution of the resilience plan.
- Incident Response Communication – communication strategy (what, when, who and to whom) with communication outlines or templates.
- Data Recovery / Restoration Platform Deployment – runbooks for data recovery, Restoration Platform deployment, testing and operations .
- Critical Service Delivery (per service) – service overview (functionality and limitations), pre-agreements and authorizations, operation playbooks (including screenshots) to operate service on the Restoration Platform.
- Transition to Normal Operations - approach and timeline, runbooks for extracting transition activity from the Restoration Platform, processing it in the recovered production system, testing and resumption of normal operations.

Financial entities are required to train their personnel (technology, operations and business delivery) to activate and execute the resilience plan within the defined ouage tolerance.

Sheltered Harbor standards specify multiple control objectives (with illustrative contols) that should be met as part of the Resilience Planning. The standards prescribe regular (at least annual) tests of the plan. The tests include system testing of technology components and at least tabletop exercises for operational / business components of the plan.

Financial institutions can apply for Sheltered Harbor Resilience Certification to assure internal and external stakeholders, including regulators, of adequate operational resilience. To do so, the financial entity will need to have an independent audit/review to confirm the completeness of its Resilience Plan as well as tests and regular exercises to demonstrate its ability to promptly resume critical services after a severe outage.

Implementation Roadmaps

Since DORA's ICT Management Standards apply to all ICT risks and financial institutions have limited resources, DORA's implementation guidelines recommend the use of risk-based prioritization:

- Focus first on **critica**l services, data, and ICT systems.
- Consider risk exposure / vulnerability of these critical items.

Critical data risks and critical business services outages addressed by Sheltered Harbor should be the initial focus of implementating DORA ICT Risk Management standards.

Below is the roadmap for the implementation of ICT Risk Management standards recomended by DORA compared with Sheltered Harbor's implementation guidance.

Phase 1 – Gap Analysis & Governance Setup

The objective of this phase in both frameworks (DORA and Sheltered Harbor) is to establish governance, scope, and assess current state. Both recommend steps like assigning responsibility to a management body for the program (board-level accountability), setting up a cross-functional risk committee, conducting gap analysis, defining critical business services (critical and important functions), and developing an

implementation roadmap and budget. Sheltered Harbor's framework furthermore offers tools, such as Sheltered Harbor's Maturity Model for Severe Outages, to enable a gap analysis focused on data risks and critical services outages.

Phase 2 – Risk Identification & Classification

The objective of both frameworks is to build inventory and classify ICT risks, but Sheltered Harbor is focused on risks causing critical data loss and prolonged outages of critical services. To this extent Sheltered Harbor requires identification of critical data backups that include data (business and application/system configurations) that will require enhanced cyber protection. Furthermore, it requires to identify critical ICT systems (applications, databases, operating systems, servers, cloud and other third-party services) that support time-sensitive critical services (services with outage tolerances shorter than maximum duration of recovery to normal operations under severe scenario).

Phase 3 – Protection & Prevention Controls

The DORA objective for this phase is to implement baseline safeguards (security policies, preventive controls, change and patch management processes. Sheltered Harbor is not focused on protection and prevention of operational systems, but does require that the *Restoration Platform* incorporate baseline safeguards.

Phase 4 – Detection & Response

Both frameworks seek to ensure incidents are detected and managed effectively, but Sheltered Harbor is focused specifically on severe outages of time-sensitive critical business services. To this extent it asks financial institutions to follow Sheltered Harbor standards to complete the following steps:

1. Detect and escalate potentially prolonged outages of time-sensitive critical business services.
2. Implement a transitional *Restoration Platform*.
3. Identify critical data backups required to deploy/operate the *Restoration Platform.*
4. Implement a Vaulting Process to store critical data backups.
5. Conduct the data recovery test and implementation review of the Vaulting Process.

6. Develop a Sheltered Harbor *Resilience Plan.*
7. Train staff on prompt resumption of critical business services in accordance with the *Resilience Plan.*
8. Conduct resilience readiness tests.
9. (Optional) Conduct an independent audit / review of the Vaulting Process and receive Sheltered Harbor *Vaulting Process Certification.*
10. (Optional) Conduct an independent audit / review of the Resilience Plan and receive Sheltered Harbor *Resilience Certification*.

Phase 5 – Recovery & Learning

The objective of both frameworks is to build resilience for restoration after ICT incidents, but Sheltered Harbor is focused specifically on incidents resulting in loss of critical data. To this extent it asks financial institutions to follow Sheltered Harbor standards to complete the following steps:

1. Expand the Vaulting Process to include all critical data backups.
2. Prepare to quickly resume operations on a temporary *Restoration Platform.*
3. Develop a fail-back process to update the recovered data with transactions from the Restoration Platform.
4. Update DR plans to source critical data backups from the cyber-resilient data vault and to adjust it for transitional activity.
5. Conduct updated disaster recovery (DR) testing.

Note: Financial Entities may decide to switch the order of implementation of Phases 4 and 5 or skip Sheltered Harbor Resilience to critical services outages altogether. In this case, Phase 5 should include implementation of the Vaulting Process.

Phase 6 – Continuous Improvement & Oversight

The objective of both frameworks is to sustain compliance and resilience, but Sheltered Harbor is focused specifically on incidents resulting in loss of critical data and severe outages of time-sensitive critical business services. Sheltered Harbor recommends that financial institutions should conduct annual re-certification of the Vaulting Process and the Resilience Plan with required testing and control reviews/audits.

Sheltered Harbor Certifications

At their core, both DORA and Sheltered Harbor are mitigation control frameworks for addressing current and future cyber-related risks to a firm's operations. Whether by regulation (DORA) or by recommendation (Sheltered Harbor), both advocate the implementation of mitigations necessary to address risks to the delivery of financial services. Here, we will look closer at the main characteristics of these frameworks, with the objective of demonstrating that the implementation of the Sheltered Harbor approach supports DORA's regulatory requirements and enable a financial institution to make quicker progress on one of its highest risk areas – that being preparations to promptly resume critical services even after a devastating disruption.

Controls and Safeguards

DORA mandates robust controls and safeguards for financial institutions to ensure they can withstand, respond to, and recover from ICT-related disruptions. Controls and safeguards are subject to management oversight and independent joint ESA examinations. Internal controls are structured around specific ICT/RTS requirements for implementing a comprehensive framework for digital operational resilience.

Sheltered Harbor defines a standard set of control objectives that must be reviewed/ audited by an independent party to ensure the effectiveness of the control environment. Data vaulting and resilience planning must meet a set of comprehensive criteria and must include management's assertion on the effectiveness of internal controls in order to attain formal certification.

The control objectives required by Sheltered Harbor align neatly to DORA ICT standards in support of resilience.

Audits / Examinations

Independent examinations are included in DORA Articles 39 and 40. The Lead Overseer (auditor), assisted by a joint examination team, can demand documents, investigate, and inspect premises but must notify relevant authorities and the Joint Oversight Network (JON) before taking action. After their investigation, they must issue recommendations within three months.

Independent annual audits are required by a Sheltered Harbor Qualified Assessor, as part of the criteria for achieving Sheltered Harbor certification. Audit report results and recommendations are shared with management and Sheltered Harbor.

The scope and coverage prescribed by the independent Sheltered Harbor audits are comprehensive. These audits can provide a solid foundation and starting point, along with offering potential reliance for the DORA examinations.

Certification

DORA does not award certification to financial institutions, overall, DORA compliance is demonstrated through meeting the regulation's specific requirements, with ongoing oversight from EU authorities, and subject to joint examinations by ESAs. (DORA validation-related certifications are offered at organizational / individual levels: Compliance Offices, Practitioner and Lead Auditor (examiner).)

Sheltered Harbor Certification supports the effectiveness of Resilience to internal and external parties including regulators and examiners. Sheltered Harbor provides evidence based certification that supports cyber-resilient data vaulting; and overall preparation for prompt recovery of critical services from a severe outage.

EU financial institutions that achieve Sheltered Harbor certification attain comfort that controls, safeguards and ICT compliance requirements exist and align to key DORA ICT standards.

In today's rapidly evolving threat landscape, regulatory compliance regarding data protection, data portability, and the prompt resumption of critical business services after a severe disruption, is paramount for financial institutions. Financial institutions that implement Sheltered Harbor's standards will be well-positioned to provide auditable evidence and practical readiness for DORA requirements involving data resilience, business continuity, and disaster recovery preparedness.

Where you can learn more

Visit https://ShelteredHarbor.org to learn more about Sheltered Harbor. Participation in Sheltered Harbor is open to financial record keepers of all types. Join on our website now.

In-depth preparation materials (Specifications and Guides) are available to Sheltered Harbor Participants and select Alliance Partners who provide the services, and solutions necessary to help financial entities implement Sheltered Harbor's resilience standards.

Shelterted Harbor Participants looking to get started with their risk assessment should request a workshop and download the Sheltered Harbor Maturity Model; DORA mapping; and additional information from the Sheltered Harbor content portal.