

DORA PREPARATION CHECKLIST

The following checklist serves as a high-level guide on what to address to help clients prepare for the Digital Operational Resiliency Act (DORA). The following checklist is not a substitute for a risk assessment or other actions required by DORA. Contact a Drawbridge account manager or representative to learn more about cybersecurity measures that meet DORA requirements.

CHECKLIST ITEMS FOR DORA COMPLIANCE	YES	NO
Review and document at least once a year: strategies, policies, procedures, and tools that are necessary to duly and adequately protect all information assets.	<input type="checkbox"/>	<input type="checkbox"/>
Ensure the cyber risk management shall be subject to an internal audit at least once a year. Those auditors shall possess sufficient knowledge, skills, and expertise in Information & Communication Technology (ICT) risk, as well as appropriate independence	<input type="checkbox"/>	<input type="checkbox"/>
Verify your policies include at least the following equivalent requirement: Information Security Policy, Access Restriction Policies, Authentication and Encryption Policies, ICT Change Management Policies, Patch and Update Policies.	<input type="checkbox"/>	<input type="checkbox"/>
Have a comprehensive Business Continuity Plan/Policy (BCP) and periodically test the response and recovery plans supporting all functions at least yearly	<input type="checkbox"/>	<input type="checkbox"/>
Establish and implement a cybersecurity incident management process to detect, manage, and notify of incidents.	<input type="checkbox"/>	<input type="checkbox"/>
Ensure there are sufficient resources and capabilities to monitor user activity, the occurrence of anomalies, and ICT related incidents, in particular cyber attacks	<input type="checkbox"/>	<input type="checkbox"/>
On a continuous basis, identify all sources of ICT risk and assess cyber threats and ICT vulnerabilities relevant to them	<input type="checkbox"/>	<input type="checkbox"/>
Identify and document all processes that are dependent on Information and Communication Technology (ICT) third-party service providers and record in your "Register of Information".	<input type="checkbox"/>	<input type="checkbox"/>
Establish and follow procedures to identify and assess all relevant risks in relation to the contractual arrangement with ICT third-party service providers and that they comply with appropriate information security standards	<input type="checkbox"/>	<input type="checkbox"/>
Implement backup policies and procedures specifying the scope of the data that is subject to the backup and the minimum frequency of the backup. Document and test all restoration and recovery procedures and methods	<input type="checkbox"/>	<input type="checkbox"/>
Perform appropriate tests, such as vulnerability assessments, technical security assessments, and penetration testing on all systems supporting critical functions.	<input type="checkbox"/>	<input type="checkbox"/>
Construct security awareness programmes and digital operational resilience training as compulsory modules in your staff training schemesvvv	<input type="checkbox"/>	<input type="checkbox"/>

## NEXT STEPS

Contact a Drawbridge representative to learn more about the steps your firm needs to take to meet DORA requirements. Email us at [info@drawbridgeco.com](mailto:info@drawbridgeco.com).

## LOCATIONS

### USA:

#### Florida:

+1 561 - 593 - 1600

#### New York, NY

+1 646 - 907 - 5660

#### Denver, CO

+1 646 - 907 - 5660

### EMEA:

#### London, UK

+44 ( 0 ) 208 078 8825



### About Drawbridge

Drawbridge delivers independent cybersecurity oversight, blending cutting-edge technology with industry expertise. We help the investment sector turn cybersecurity into a strategic advantage. Serving over 1,200 global clients, we provide tailored solutions that meet the financial industry's highest security and regulatory standards, empowering boards, investors, and regulators with confidence. Our mission is to protect your reputation, systems, and data, keeping you ahead of evolving cyber threats and compliance requirements.

 [info@drawbridgeco.com](mailto:info@drawbridgeco.com)

 [drawbridgepartnersllc](https://www.linkedin.com/company/drawbridgepartnersllc)

 [@DrawbridgeCyber](https://twitter.com/DrawbridgeCyber)

### Disclaimer

©2025 Drawbridge Partners, LLC. All rights reserved. Unauthorized reproduction, distribution, or use of this material or any part of its contents is strictly prohibited without the prior written consent of Drawbridge.

The information contained in this material is provided by Drawbridge Partners, LLC and/or any of its affiliates (collectively, "Drawbridge") for informational purposes only. Nothing contained herein shall constitute legal, regulatory, investment, financial, or professional advice, nor shall anything contained herein be construed as a recommendation, reference, or endorsement by Drawbridge. Drawbridge makes no representations or warranties of any kind, express or implied, including but not limited to, any warranties related to the completeness, accuracy, reliability, suitability, or availability with respect to the information, products, services, or related graphics contained in this material for any purpose. No reliance shall be placed on any information contained herein. By reviewing this material, you acknowledge that neither Drawbridge nor any of its third-party providers shall under any circumstance be liable for any lost profits or lost opportunity, direct, indirect, special, consequential, incidental, or punitive damages whatsoever, even if Drawbridge or its third-party providers have been advised of the possibility of such damages.

This material may contain links to other websites which are not under the control of Drawbridge.

Drawbridge has no control over the nature, content, and availability of those sites.

The inclusion of any links does not imply a recommendation, nor does it endorse the views expressed within them. Drawbridge reserves the right to make additions, deletions, or modifications to the contents of this material at any time without prior notice.