INTAPP CUSTOMER GUIDE:

DIGITAL OPERATIONAL RESILIENCE ACT

Published – June 2025

1. Introduction

The EU Digital Operational Resilience Act (**DORA**) applies to financial institutions, investment firms, fund management companies, insurance undertakings, and other financial entities regulated in the European Union (**Financial Entities**). Intapp's products and services may be used by Financial Entities either as customers or as service recipients.

One of DORA's key objectives is to strengthen operational resilience by ensuring prudent risk management of information technology and communication (ICT) services. DORA harmonizes various pre-existing EU requirements, and introduces new requirements, which indirectly impact the services provided by third party ICT service providers, such as Intapp, around the following pillars:

i. ICT risk management
ii. Incident management and reporting
iii. ICT third party risk management

Under DORA, Financial Entities must apply certain of these requirements, such as ICT third party risk management, in light of the principle of proportionality, taking into account the nature, scale, complexity and importance of third-party ICT services. This is a key principle that applies when considering how Intapp's products and services can support a Financial Entity's digital operational resilience.

Intapp is committed to building a comprehensive program that builds resilience in its products and services and the capability for continuous operations across its products and services.

2. Purpose

This guide (this **Guide**) provides an overview of how Intapp's products and services facilitate compliance with DORA. This Guide may be utilised as part of a Financial Entity's digital operational resilience training with regard to its use of Intapp's products or services.

3. ICT Risk Management

In order to maintain full control over ICT risk, DORA requires Financial Entities to have comprehensive capabilities to enable strong and effective ICT risk management. Third-party ICT service providers such as Intapp can be an important component of a Financial Entity's overall ICT landscape, particularly where supporting any critical or important functions of the Financial Entity.

How Intapp facilitates compliance

☑ **Secure Solution:** Intapp provides its customers with a secure solution that provides confidentiality, integrity and availability for each customer's data. Security compliance certifications are vital for enforcing strong information security measures and proving adherence to industry standards. By being certified, we show our dedication to robust security protocols and risk management; Intapp is certified under ISO 27001, 27017, 27018 and 27701 and uses external auditors to verify the adequacy of its security measures, including by SOC 2 reports. Intapp's ICT risk management controls for its products and systems include logical and physical access controls, encryption and cryptographic controls, monitoring of system performance and capacity demand controls through Intapp's hosting providers, change management procedures and appropriate risk mitigation activities for risks arising from potential business disruption. Intapp undertakes rigorous testing of its products and systems. Further information on Intapp's security measures and vulnerability management policy is available at: https://www.intapp.com/cloud/security/

☑ **Secure Cloud Adoption:** In addition, Intapp maintains cloud policies that provide the critical governance framework required for secure cloud adoption. These policies define controls, roles and processes required to manage products and data, allowing firms to fully leverage the cloud infrastructure while mitigating risks. Intapp regularly reviews and (where appropriate) updates the cloud policies to ensure they align with evolving security threats, regulatory changes, and advancements in cloud technologies. Further information is available at: https://www.intapp.com/cloud/policies/.

☑ **Assessing Vulnerabilities**: Intapp has a documented secure development process that is designed to prevent and detect security vulnerabilities before an insecure component is deployed or released. Where we find that a vulnerability is affecting our products, including vulnerabilities detected in third-party components we use, we have multiple controls in place. Intapp accepts reports for vulnerabilities through all possible channels. Further information on Intapp's vulnerability management policy is available at: https://www.intapp.com/cloud/security/

☑ **Business Continuity Planning:** Intapp is committed to developing a comprehensive Business Continuity Management program that builds resilience and the capability for continuous operations across its operations and departments despite various disruptions. Intapp's framework leverages industry best practices, including those found at https://www.intapp.com/cloud/security/. These standards are designed to ensure a comprehensive, structured, and internationally recognized approach to business continuity. For additional details regarding Intapp's Business Continuity Policy, please reach out to your Account Executive.

☑ **Intapp Staff Training:** In addition, training is provided to Intapp employees, such as annual security awareness training programs, knowledge-sharing sessions, and dissemination of best practices to empower employees to cultivate a strong cloud security culture within Intapp. Intapp staff in key roles also participate in annual training and awareness initiatives aligned specifically with Intapp's Business Continuity (BC) program. These include professionally facilitated tabletop exercises and knowledge-sharing sessions led by personnel who are certified through the Disaster Recovery Institute (DRI). Training topics include the restoration of critical business functions, crisis management, and operational continuity with tier-1 suppliers. The program is overseen by Intapp's BC governance committee, which regularly reviews and supports training efforts across the organization.

4. Incident Management and Reporting

For Financial Entities, the ability to identify, investigate, and manage ICT-related incidents is an essential pillar for addressing cyber risk throughout supply chains, and is not just a regulatory requirement.

Intapp has operationalized its notification of ICT-related incidents, and related assistance, so as to ensure that Financial Entities can meet their regulatory obligations under DORA while balancing what is operationally feasible across Intapp's customer base.

How Intapp facilitates compliance

☑ **Direct Notification:** Intapp commits to notifying customers without undue delay in respect of accidental or unlawful loss, access or disclosure of the customer's data, and investigating and providing updates on its remedial or mitigation measures, in accordance with Intapp's security terms available at: https://www.intapp.com/cloud/security/ .

☑ **Intapp Status Page:** Intapp will notify of ICT-related incidents that do not involve a data breach by posting notifications and updates (including root-cause analyses where appropriate) at the Intapp Status Page, available at: https://status.my.intapp.com.

5. ICT Third Party Risk Management

Under DORA, Financial Entities must comply with certain key principles in the management of third-party ICT risk, which are of particular importance when an ICT third-party service provider supports a Financial Entity's critical or important functions. Those principles are reflected within contractual terms that DORA expects Financial Entities to have in place with their third-party ICT service providers, covering, among other areas, service levels, data security, audit and access rights, regulatory co-operation, termination and exit provisions, business continuity planning, and sub-contracting of ICT services that support critical or important functions.

Intapp has developed a set of streamlined contractual terms that comply with the requirements under DORA, as well as expectations of EU regulators in respect of outsourcings of critical of important functions. These are contained in Intapp's customer agreements.

How Intapp facilitates compliance

☑ **DORA Compliant Customer Agreements**: Intapp's security commitments set forth in its current Master Subscription and Services Agreement and Data Processing Agreement are designed to help clients meet their DORA commitments.

☑ **Supporting Registers of Information**: Intapp will provide key information necessary for Financial Entity customers to complete their registers of information.

☑ **Supply Chain Resilience**: Intapp is committed to overseeing any subcontractors for its products and services and ensuring that it has in place appropriate contract terms with its subcontractors so as to enable Intapp's compliance with its obligations to each Financial Entity customer. Under DORA, particular focus is placed on subcontractors that effectively underpin ICT services that support critical or important functions. Intapp identifies for its customers those "critical" subcontractors whose services effectively underpin each applicable Intapp product or service, available at: https://www.intapp.com/sub-processors/DORA/.