Integrated Control Framework

This document presents the contents of our Integrated Control Framework. For your convenience, we have mapped the ISO 27001:2022 Annex A and DORA[1] requirements[2] to this framework. The purpose of this document is to inform you about the controls we have implemented and demonstrate how they meet the ISO and DORA standards' requirements.

[1] DORA: Digital Operational Resilience Act

[2] We mapped our ICF with the requirements from "Regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework" (referred to in the overview as RTS) and the "Digital Operational Resilience Act" (referred to in the overview as DORA).

ICF Domain	Control Objective	Control ID	Control Description	ISO27001 Annex A Controls	DORA requirements
01. Organization, Direction and Policies	01.1 Controls provide reasonable assurance that roles and responsibilities are defined, and processes and governance structures are designed, implemented and evaluated.	1.1.1 Governance structure	A governance structure is in place to coordinate information security, privacy and business alignment. This structure ensures that information security and privacy policies, standards and procedures are reviewed periodically or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5.2: Information security roles and responsibilities	Article 2: General elements of ICT security policies, RTS
		1.1.2 Periodic risk assessments	Periodically, risk assessments are updated and reacted accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	Clause 6.1.2: Information security risk assessment	Article 3: ICT risk management, RTS
		1.1.3 Review of control frameworks	Periodically, cybersecurity and privacy governance controls are reviewed and approved by management, and communicated to personnel througout the internal network.	Not part of ISO	Article 27: Format and content, RTS
		1.1.4 Review of Risk Management policy	Periodically, the Risk Management Policy and procedure is reviewed and updated if necessary.	5.1: Policies for information security	Not part of DORA
		1.1.5 Review of Privacy policy	Periodically, the Data Privacy Policy and the Data Privacy Organization is reviewed and updated if necessary.	5.1: Policies for information security 5.34: Privacy and protection of personal identifiable information (PII)	Not part of DORA
		1.1.6 Contact with relevant law enforcement, regulatory bodies and associations	Periodically, appropriate contacts within relevant law enforcement, regulatory bodies and associations within cybersecurity and privacy are reviewed.	5.6: Contact with special interest groups	Not part of DORA
		1.1.7 Security Policy	Periodically, the security policies are reviewed and updated if necessary.	5.1: Policies for information security	Article 2: General elements of ICT security policies, RTS

ICF Domain	Control Objective	Control ID	Control Description	ISO27001 Annex A Controls	DORA requirements
02. Access Controls	02.1 Controls provide reasonable assurance that, based on job responsibilities, only authorized persons have logical access to resources of products in scope and appropriate authenticity means are in place	2.1.1 Access management procedure	Periodically, the policy for identification and access management is reviewed and updated if necessary.	5.1: Policies for information security, 5.15: Access control	Article 20: Identity management, RTS Article 21: Access control, RTS
		2.1.2 User registration and de-registration process	Periodically, the formal user registration and de-registration process that governs the assignment of access rights is documented and approved.	5.1: Policies for information security, 5.16: Identity management, 5.18: Access rights, 8.2: Privileged access rights	
		2.1.3 Review of privileged accounts	Periodically, privileged access rights for users and services are reviewed according to the access management procedures.	8.2: Privileged access rights	
		2.1.4 Disabling privileged accounts	Periodically, the disabling of inactive privileged accounts after an organization-defined time period, is reviewed. Deficiencies are followed up.	5.18: Access rights	
		2.1.5 Password Policy	Adherence to existing Password Policy is checked at least annually for Exact users and service accounts to enforce complexity, length and passwords duration products in scope.	5.15: Access control, 5.17: Authentication information, 5.36: Compliance with policies, rules and standards for information security	
	02.2 Controls provide reasonable assurance that logging is protected and monitored	2.2.1 Logging procedure	Periodically, the process regarding the collection, review and analyses of logs is reviewed and updated.	8.15: Logging, 8.16: Monitoring activities	Article 12: Logging, RTS
		2.2.2 Log protection	Periodically, the protection of event logs and audit tools from unauthorized access, modification and deletion is reviewed. Deficiencies are followed up.	8.15: Logging, 8.16: Monitoring activities	
		2.2.3 Log review on privileged access	Periodically, the logging of access of users and/or services with elevated privileges is reviewed. Deficiencies are followed up.	8.15: Logging, 8.16: Monitoring activities	

ICF Domain	Control Objective	Control ID	Control Description	ISO27001 Annex A Controls	DORA requirements
03. Asset Management	03.1 Controls provide reasonable assurance assets are properly managed throughout the lifecycle of the asset, from procurement through disposal, ensuring only authorized devices are allowed to access the organization's network and to protect the organization	3.1.1 Compliance Asset Management policy	Periodically, the adherence to the KPI's defined in the asset management policy, is reviewed. Deficiencies are followed up.	5.9: Inventory of information and other associated assets	Article 4: ICT asset management policy, RTS, Article 5: ICT asset management procedure. RTS, Article 11: Data and system security, RTS, Article 14: Securing information in transit, RTS
		3.1.2 Secure data transport procedure	Periodically, operational procedures to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures, are reviewed and updated if necessary.	5.1: Policies for information security, 7.10: Storage media, 8.24: Use of cryptography	
		3.1.3 Secure disposal of assets	Periodically, secure disposal, destruction or reuse of system components according to the asset management policy to prevent information being recovered from these components, is reviewed. Deficiencies are followed up.	7.1: Physical security perimeters	
		3.1.4 Return devices policy compliance	Periodically, operational procedures to determine that all Exact IT assets are returned by employees leaving Exact and that these assets do not contain any old information, is reviewed. Deficiencies are followed up.	5.9: Inventory of information and other associated assets, 5.11: Return of assets	
04. Business Continuity	04.1 Controls provide reasonable assurance that operations can continue and contracted services can be provided to customers.	4.1.1 BCM policy and procedures	Periodically, management reviews and updates (i) the local procedures for recovery of business critical processes (BCM) in a crisis situation, and (ii) the back-up procedures and retention schedules in line with the corporate BCM policy and guidelines The documents are available to staff through the organization's intranet.	5.29: Information security during disruption, 5.30: ICT readiness for business continuity, 8.14 Redundancy of information processing facilities	Article 24: Components of the ICT business continuity policy, RTS, Article 26: ICT response and recovery plans, RTS
		4.1.2 Business Continuity Test	Periodically, business continuity tests are performed to safeguard business continuation in case of crisis situations. Deficiencies are followed up.	5.29: Information security during disruption, 5.30: ICT readiness for business continuity, 8.14 Redundancy of information processing facilities	Article 25: Testing of the ICT business continuity plans, RTS
		4.1.3 Back-up and restore	Periodically, backup files are created of the relevant (customer) data and applications and the restore is tested.	8.13: Information backup	Article 8: Policies and procedures for ICT operations, RTS

ICF Domain	Control Objective	Control ID	Control Description	ISO27001 Annex A Controls	DORA requirements
05. Communi-cations Security	05.1 Controls provide reasonable assurance that integrity, availability and confidentiality of the data, systems, applications or services can be provided.	5.1.1 Secure Network Design	Periodically it is reviewed, whether basic architectural concepts of network security controls are embedded in the architectural design. Network segmentation and De-Militarized Zones are in place to separate untrusted networks from trusted networks.	8.20: Networks security, 8.21: Security of network services, 8.22: Segregation in networks	Article 13: Network security management, RTS
		5.1.3 Boundary protection	Periodically, the external network boundary and at key internal boundaries within the network are monitored and controlled by firewall, router management.	8.20: Networks security, 8.21: Security of network services	
06. Compliance	06.1 Controls provide reasonable assurance that risks relating to breaches of any law, statutory, regulatory or contractual obligations are addressed.	6.1.1 Developments in local legislations	Periodically, it is assessed if the relevant legislatives developments in the countries we operate have been sufficiently incorporated into company policies and our terms & conditions.	5.31: Legal, statutory, regulatory and contractual requirements, 5.32: Intellectual property rights	Article 13: Learning and evolving, DORA
		6.1.2 Operational processes and governance	Periodically, (operational) managers review the processes and documented procedures within their area of responsibility to adhere to appropriate security policies, standards and other applicable requirements. Documents are updated if necessary.	5.37: Documented operating procedures, 5.1: Policies for information security, 5.9: Inventory of information and other associated assets, 8.32: Change management	Article 2: General elements of ICT security policies, RTS
	06.2 Controls provide reasonable assurance that non-compliance with the control framework is timely identified, assessed and addressed	6.2.1 Risk and control framework review	Periodically, the GRC team reports to the governance committee about the risks and effectiveness of control framework. ISMS owners are informed about the control execution of corporate controls for their assessment of the impact for their ISMS.	Not part of ISO	Article 3: ICT risk management, RTS
		6.2.2 Follow-up on deficiencies	Periodically, the procedure to respond to findings from security and privacy assessments, risk assessment, incidents and audits (to ensure proper remediation has been performed), is reviewed and updated if necessary.	5.24: Information security incident management planning and preparation, 5.25: Assessment and decision on information security events, 5.26: Response to information security incidents, 5.27: Learning from information security incidents, 5.28: Collection of evidence, 6.8 Information security event reporting	

ICF Domain	Control Objective	Control ID	Control Description	ISO27001 Annex A Controls	DORA requirements
07. Crypto-graphy	07.1 Controls provide reasonable assurance that the confidentiality of the organization's data is ensured through implementing appropriate cryptographic technologies to protect systems and data.	7.1.1 Cryptographic standards	The cryptographic standards are included in Exact's security policy. This security policy is reviewed annually by management.	5.1: Policies for information security	Article 6: Encryption and cryptographic controls, RTS
		7.1.2 Cryptographic transport controls	Periodically, the execution of cryptographic mechanisms which are in place to protect the confidentiality, integrity of sensitive data being transmitted, are monitored.	5.14: Information transfer, 8.24: Use of cryptography	
		7.1.3 Cryptographic storage controls	Periodically, cryptographic controls which are in place to prevent unauthorized disclosure of sensitive data at rest (e.g. disk encryption of server and workstation level), are monitored.	5.14: Information transfer, 8.24: Use of cryptography	
		7.1.4 Cryptographic key management	Periodically, controls which are in place for cryptographic key management to protect the confidentiality, integrity and availability of keys, are monitored. Deficiencies are followed up.	8.24: Use of cryptography	Article 7: Cryptographic key management, RTS

ICF Domain	Control Objective	Control ID	Control Description	ISO27001 Annex A Controls	DORA requirements
08. Human Resource Security	08.1 Controls provide reasonable assurance that employees and contractors are suitable for their roles in terms of their capabilities, are aware of their responsibilities and that they are hired, transferred, and leave Exact in line with HR procedures	8.1.1 Job House review	Periodically it is evaluated whether all changes to the job house been approved by the CHRO.	5.3: Segregation Of duties	Article 19: Human resources policy, RTS
		8.1.2 Inflow and Outflow procedures	A set of centralized HR policies and procedures for hiring personnel. internal transfer and employing contractors and termination of employment is maintained. Policies and procedures are evaluated by management periodically.	5.16: Identity management, 6.5: Responsibilities after termination or change of employment	
		8.1.3 Employment verification is monitored	Periodically, it is verified that employment verification is done in line with the policy and is monitored centrally. Exceptions will be classified and followed up.	6.1: Screening	
		8.1.4 Non Disclosure Agreements	Periodically, signing a NDA and where relevant a TPA for every contractor is centrally monitored.	5.4: Management responsibilities, 6.2: Terms and conditions of employment	
	08.2 Controls provide reasonable assurance that employees are made aware of the information security related policies and potential consequences of non-compliance	8.2.1 Security Awareness	All employees need to follow an annual security awareness training. In case employees don't complete the training in time, their access is revoked.	6.3: Information security awareness, education and training	
		8.2.2 Disciplinairy process	Periodically, the disciplinairy process for personnel failing to comply with established security policies, standards and procedures is reviewed and updated if necessary.	6.4: Disciplinary process	

ICF Domain	Control Objective	Control ID	Control Description	ISO27001 Annex A Controls	DORA requirements
09. Incident Management	09.1. Controls provide reasonable assurance that all incidents of the products and services in scope are managed, monitored and resolved effectively	9.1.1 Security Incident Management	Periodically, the Security and Privacy Incident Management policy and procedures which facilitate an organization-wide response capability for security and privacy-related incidents, are reviewed and updated if necessary.	5.24: Response to information security incidents, 5.25: Response to information security incidents, 5.26: Documenting security incidents, 5.27: Learning from information security incidents, 5.28: Collection of evidence, 6.8: Information security event reporting	Article 22: ICT related incident management policy, RTS Article 23: Anomalous activities' detection and criteria for ICT-related incidents' detection and response, RTS
10. Operations	10.1 Controls provide reasonable assurance that the organization is implementing changes in a controlled manner, managing the demand for capacity and that internal system clocks to generate time stamps for audit records cannot be tampered with.	10.1.1 Capacity Management	Periodically it is reviewed if, the capacity of servers for products in scope is monitored using tooling and - in case of irregularities, the logs are investigated and appropriate action is taken.	8.6: Capacity management	Article 9: Capacity and performance management, RTS
		10.1.2 Change management infrastructure	Periodically is reviewed if changes to the infrastructure of products in scope are executed according the the Change Management procedure. Deficiencies are followed up.	8.32: Change management	Article 17: ICT Change management, RTS
		10.1.3 Time Synchronization	Periodically, the description of time-synchronization for all critical system clocks and the implementation of the time-synchronization is reviewed and updated if necessary.	8.17: Clock synchronization	Article 12: Logging, RTS

ICF Domain	Control Objective	Control ID	Control Description	ISO27001 Annex A Controls	DORA requirements
10. Operations	10.2 Controls provide reasonable assurance that systems and endpoint devices are hardened to protect against reasonable threats to those devices and the data they store, transmit and process.	10.2.1 Security baselines	Periodically, secure baseline configurations for technology platforms in scope are reviewed, in consistency with industry-accepted system hardening standards, and updated if necessary.	5.36: Compliance with policies, rules and standards for information security	Articles 11: Data and system security, RTS Article 13: Network security management, RTS
		10.2.2 Continuously monitoring of systems	Periodically, it is assessed whether continuously monitoring of critical systems, logging and follow-up is defined and followed upon according to procedures.	5.36: Compliance with policies, rules and standards for information security, 8.15: Logging, 8.16: Monitoring activities.	
		10.2.3 Endpoint protection	Periodically, it is assessed whether continuous monitoring of critical systems, logging and follow-up is defined and followed upon according to procedures.	5.9: Inventory of information and other associated assets, 5.36: Compliance with policies, rules and standards for information security, 8.7: Protection against malware, 8.8: Management of technical vulnerabilities	
		10.2.4 Asset compliance	Periodically, assets in scope are reviewed for compliance with the organization's cybersecurity and privacy policies and standards.	5.9: Inventory of information and other associated assets, 5.15: Access control, 5.17: Authentication information, 5.36: Compliance with policies, rules and standards for information security	
		10.2.5 Antimalware for servers/containers	Periodically, antimalware for servers/containers are reviewed for compliance with the organization's cybersecurity and privacy policies and standards.	8.7: Protection against malware	Article 11: Data and system security, RTS
		10.2.6 Vulnerability management	Periodically it is reviewed if activities to protect against vulnerabilities, are executed according to the procedure for vulnerability management.	8.8: Management of technical vulnerabilities	Article 10: Vulnerability and patch management, RTS
		10.2.7 Patch management	Periodically, patch management is reviewed for compliance with the organization's cybersecurity and privacy policies and standards.	8.8: Management of technical vulnerabilities	

ICF Domain	Control Objective	Control ID	Control Description	ISO27001 Annex A Controls	DORA requirements
11. Physical and environmental security	11.1 Controls provide reasonable assurance that the organization restricts physical access to buildings and information assets to authorized personnel.	11.1.1 Cable and power management	Periodically, the physical security procedures, which protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage, is reviewed and updated if necessary.	7.12: Cabling security	Article 18: Physical and environmental security, RTS
		11.1.2 Physical Access Control Data center	Periodically, it is verified that physical access of IT assets used in data center is restricted to authorized personnel. Security perimeters (card controlled entry gates and/or manned reception desks) are used to protect the data center.	7.1: Physical security perimeters, 7.2: Physical entry, 7.3: Securing offices, rooms and facilities, 7.5: Protecting against physical and environmental threats, 7.6: Working in secure areas	
12. Supplier Relationships	12.1 Controls provide reasonable assurance that third parties adhere to requirements relevant to products and services in scope.	12.1.1 Supplier management Policy	Periodically, the Supplier Management Policy is reviewed and updated if necessary.	5.19: Information security in supplier relationships, 5.20: Addressing information security within supplier agreements, 6.6: Confidentiality or non-disclosure agreements	Article 28: Key principles for a sound management of ICT third-party risk - general principles, DORA
		12.1.2 Suppliers Contract Review	Compliance with the procurement policy is checked for new and renewed supplier contracts	5.22: Monitoring, review and change management of supplier services	
		12.1.3 Suppliers SLA / Security controls review	Periodically, the supplier service delivery for compliance with established contract agreements is reviewed.	5.22: Monitoring, review and change management of supplier services	
		12.1.4 Review assurance reports	Periodically, the assurance reports are reviewed to assess whether risks related to these services are sufficiently mitigated.	5.22: Monitoring, review and change management of supplier services	

ICF Domain	Control Objective	Control ID	Control Description	ISO27001 Annex A Controls	DORA requirements
13. System acquisition, Development and maintenance	13.1 Controls provide reasonable assurance that software changes and infrastructure-as-code changes to the application in scope are authorized and implemented completely and accurately	13.1.1 Segmentation of environments	Periodically is reviewed that development and production environments are segmented.	8.25: Secure development lifecycle, 8.31: Separation of development, test and production environments	Article 16: ICT systems acquisition, development, and maintenance, RTS
		13.1.1a Development Best Practice	Periodically, the SDLC policy is reviewed and updated if necessary and included in the development procedures of the products in scope.	8.25: Secure development lifecycle	
		13.1.3 SDLC compliance	Periodically, management reviews and evaluates the adherence of software changes to the SDLC Policy and procedures and takes appropriate actions when needed.	8.25: Secure development lifecycle, 8.32: Change management	
14. App Center Security	14.1 Controls provide reasonable assurance that 3rd party app developers only get access to data compliant for their purpose in their app integration	14.1.1 Establish and review App Center Security policy	Periodically, the App Center Security Policy, is reviewed and updated if necessary.	Not part of ISO	Not part of DORA

ICF Domain	Control Objective	Control ID	Control Description	ISO27001 Annex A Controls	DORA requirements
14. App Center Security	14.1.2 App developers approve terms and conditions	14.1.2 App developers approve terms and conditions	Periodically, the approval to terms and conditions is reviewed.	Not part of ISO	Not part of DORA
	14.1.3 Approve data and security review	14.1.3 Approve data and security review	Periodically, the approval of data and security review is analyzed.	Not part of ISO	Not part of DORA
	14.1.4 Only approved data scopes are allowed to be accessed by apps	14.1.4 Only approved data scopes are allowed to be accessed by apps	Periodically, the data scopes which are allowed to be accessed by apps are reviewed.	Not part of ISO	Not part of DORA
	14.1.5 Restrict access when terms and conditions not complied	14.1.5 Restrict access when terms and conditions not complied	Periodically, it is reviewed whether the terms and conditions are complied. Deficiencies are followed up.	Not part of ISO	Not part of DORA