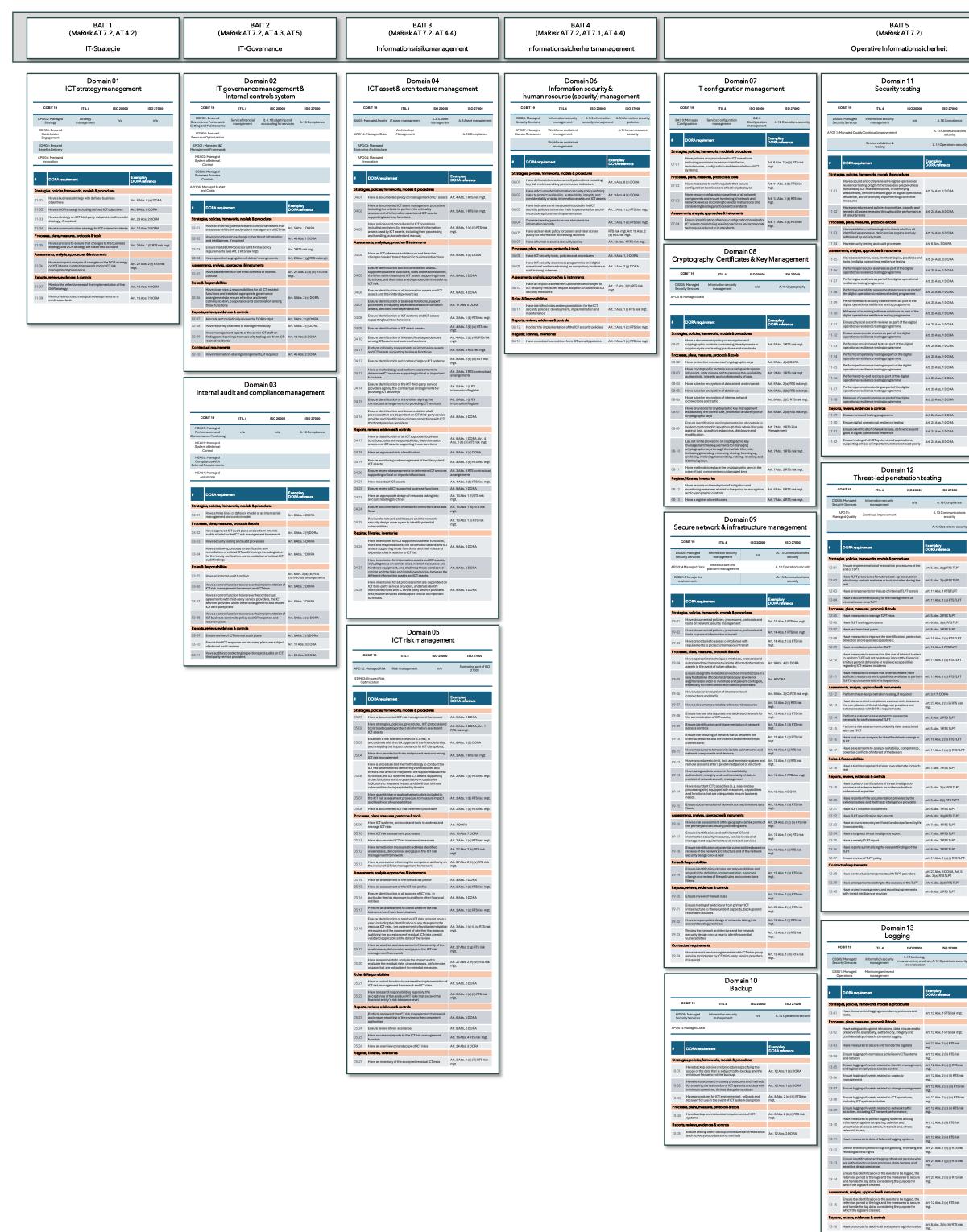
DORA DEEP DIVE: REQUIREMENTS AND DOMAIN MAPPING



		BAIT 6 (MaRisk AT 7.2, AT 4.3) Identitäts- und Rechtemanagement	BAIT7 (MaRisk AT 7.2, AT 8.2) IT-Projekte und Anwendungen	BAIT 8 (MaRisk AT 7.2) IT-Betrieb	BA (MaRis (IT-)Auslagerungen u	kAT9)	
				L			
	Domain 14 Data and ICT system security	Domain 17 Identity and access management	Domain 18 ICT change management	Domain 21 ICT incident management	Domain 23 ICT outsourcing & third-party risk management	Domain 24 Subcontracting management	I
nce ations	COBIT 19 ITIL 4 ISO 20000 ISO 27000 DSDID: Managed Bocurshy Services Information security management n/a A.18 Compliance ACP0.14 Humged Data A.13 Communications A.13 Communications	COBIT19 ITIL.4 ISO 20000 ISO 20000 DS005: Nanaged Security Services Information security management n/b A.9 Access control.	COBIT 19 ITL 4 ISO 20000 ISO 27000 BADD: Managed Organizational Change Organizational Change 0.5.1 Change management 8.5.1 Change A-14 System acquisition, development and maintenance BADD: Managed IT Change control/ Change 8.5.1 Change Maintenance	COBIT 19 ITL 4 ISO 20000 ISO 27000 Managed Service Requests and Incidents Security Services 8.6.1 hoddest management A.16 information security incident management A.16 information security incident security Services DSSOI: Managed Security Services Service request and an approximation security Services A.12 Operations security	COBIT 19 ITL 4 ISO 20000 ISO 27000 APO10. Managed Vendors Supplier managemfert wanagement 8.3.4 Supplier management A1.6 Synom development and management	COBIT 19 ITL 4 ISO 20000 ISO 27000 APC10 Managed Vendors Suppler managemfert wanagement 8.3.4 Suppler management A.1.5 Symmet Apple of the suppler management	
security	APO11: Managed Data security APO11: Managed Quality A12 Operations security DORA requirement DORA requirement	DORA requirement DORA requirements DORA requirements Strategies, policies, frameworks, models & procedures Trot New policies, procedures and control bat taddess sourd administrations Art. 9 Abb. 4 (c) DORA	Change Changes	Losob: Varlaged Service deak a. 2 service regards A.12 Operations security management A.12 Operations security Problem management security incidents BAIDB Managed Information security 8.6.3 Problem management Knowledge and Ministry and Amountain and Amountain Amountain and Amountain and Amountain Amountain Security Security Amountain Amountain Security Security Amountain Amountain Security Secu	APO11: Managed Continual improvement Continual improvement DORA requirement DORA Reference	APO09 Managed Service level management B.33 Service level management APO11: Managed Continual improvement Continual improvement DORA requirement DORA requirement	
	CONTREQUENTIAL DORArdewoo DORArdewoo Strategies policies femeworks, models & procedures 14.01 Processes, policies femeworks, models & and/CT system rescuritly Art. 11 Abs. 1 RTSrisk mgt. Processes, protocols & book	Heve policies that limit the logical access to information 17:02 assets and CTassets to what is required for legitimate and approved functions and activities only Art. 9 Abz. 4 (c) DORA 17:03 Heve a documented policy on control of access mgmern rights mg	B DORArequirement Branshiny DORArequirement Strategies, policies, frameworks, models & procedures	Monitoring and event 9. Performances management measures and evaluation Measurement and reporting Problem management	Strategias, policies, frameworks, models & procedures and the status of	Processe, plans, messures, protocols & tools Ensure that CT third party service provident date 2401 diligner processes is able to select appropriate ICT subcontractions as required Ensure merication of contentnal amountements in	
	Here safegaards against bitwisisms, shab misute and to Art. 3 Abs. 1 RTS risk mgt. 14.02 confidentiality of data Art. 3 Abs. 1 RTS risk mgt. 14.03 Here safegaards and the single status of the single stat	Have documented identify management policies and procedure ensuming identification and submitciation of entities' information Art. 20 Abs. 1 RTSrisk mgt. 17:04 antibes' information Art. 20 Abs. 1 RTSrisk mgt. 17:05 or twole accessing the framework of the second transfer information Art. 21 Abs. 1 (PITSrisk mgt. 17:05 or twole accessing the framework of user and generic accounts, mgt. Art. 21 Abs. 1 (PITSrisk mgt.	1801 Heve documented policies, procedures and controls for LCT change management 1802 Heve documented CT change management procedures 1803 Heve following model	Knowledge management DORArequirement DORArequirement DORArequirement DORArequirement Strategies, policies, familyworks, models & procedures	Initid pany any cope providers Initid pany any cope providers 23 03 Have exit strategies and termination processes Art. 28 Abs. 8 DORA Processe, plan, measure, periodola Stobi Initid pany any control for the periodola strategies 23 04 Abse audit plants for VCT Third; pany service providers and Ant. 28 Abs. 6 DORA	Ensure replication of contractial arrangements in party service provider and subcontractors Art. 3 Abs. 1 (c) RTS Assessments, analysis, approaches & instruments Have subcontractor in subcontractor in subcontractors Art. 3 Abs. 1 (c) RTS Assessments, analysis, approaches & instruments Have subcontractor in subcontractor in subcontractor in subcontractors Subcontractor in subcontractor in subcontractors Subcontractoring	
	14:04 Here security measures against misicilica codes Art. 11 Abs. 2 (d) FITS risk mg. 14:06 Here security measures tensus that only suthinized data songer mdds, 7 (c) risk mean and religionity for the risk mg. Int 13 Abs. 2 (d) FITS risk mg. 14:05 Here security measures to risk mg. Int 13 Abs. 2 (d) FITS risk mg. 14:05 Here security measures to risk mg. Int 13 Abs. 2 (d) FITS risk mg. 14:05 Here security measures to risk mg. Art. 11 Abs. 2 (d) FITS risk mg.	17:00 Here policies and protocols for strong surfamilic sation Art. 9 Abs. 4 (d) DCRA Processes, plan, massure, protocols & book Social satisfies and strong surfamiliant satisfies and surfamiliant satisfies and surfamiliant satisfies and strong surfamiliant satisfies and metal satisfies at metal satisfies at metal	18:04 Here procedures, subtoch and footion manage Art. 17 Abs. 2 (I) RTS risk mgt. 18:04 Here procedures to document, re-evaluates, assess and epprove emigrancy changes including vorkamunds and mgt. Art. 17 Abs. 2 (g) RTS risk mgt.	21:01 offsy Art. 22 Abs. 1 R1S risk mgt. 21:02 Have a communic ation strategy for ICT related incidents. Art. 62 Abs. 8 (h) DORA Have procedures and processes to inner as a consistent of the incident and incidents. Art. 64 Abs. 8 (h) DORA 21:02 Have a communic ation strategy for ICT related incidents. Art. 52 Abs. 1 R1S risk mgt. 21:02 Have a communic ation strategy for ICT related incidents. Art. 52 Abs. 2 DORA	23:05 Have documented exitplens Art. 28 Abs. 8 DORA 23:06 Have transition plans to alternative ICT third party Art. 28 Abs. 8 DORA 23:06 Have contrigency measures to maintain business Art. 28 Abs. 8 DORA 23:07 control programmers to maintain business Art. 28 Abs. 8 DORA	Provider Perform third-party assessments on ICT third-party service provider due dilignoce processes to ensure an Perform third-party assessments on transments Perform third-party assessments on transments performance Perform third-party assessments are usure appropriate Perform third-party assessments to ensure appropriate Performance Performanc	
	14 0.6 portable employing devices and private non-portable mgt. 14 0.7 New space/in pressures to ensure the authorization to we exclude 17 in the second provide over any environment of the second seco	accounts To Enume savignment of access rights to ICT assets based on more storkwork, need to use and least prividge prioricipels, including for more and emergency access rights To T	Processes, plan, measures, protocols & tools Market Have an overall charge management process and crit Art. 9 Abs. 4 (e) DORA Have an ICT charge management process ensuring that all changes to ICT systems are recorded, tested, 1870 Art. 9 DORA	Identified, documented and addressed in order to prevent the occurrence of auch incidents. Have procedure to identify, track, log categorize and and severity and according to the criticality of the and severity and according to the criticality of the	Inappropriate of table provision of ICT territors 23.06 May one measures for the sound management of ICT thirds 23.07 May one measures to biothymer and management of ICT thirds 23.09 CT the measures to biothymer and management biothymer and management biothymer and management biothymer and management and the sound	Perform third-party assessments on replication of relevant contractual annagements in the autoontacting provide and its autoontaction. If 21 third party andre is provide and its autoontaction Perform third party assessments to ensure that the ICT Art. 3 Abs. 1 td RTS	
	14-0.0 premisses or stored externally 14-0.0 premisses or stored externally displace of decommission of data storage divides present on premisses or stored data storage divides present on premission of the stored data storage of the stored and a stored mg. Art. 1 Abs. 2 (h) RTS risk mg. 14-10 How security measures to prevent data loss and data of to CT by them and endpoint davies. Art. 1 Abs. 2 (h) RTS risk mg.	17.10 Here submated buildings for the privileged access Art, 21 Abs. 1 (e) (ii) RTS risk mg. 17.11 Ensum revelving of access rights without undus deby in the mg. Art, 21 Abs. 1 (e) (iii) RTS risk mg. 17.11 Ensum revelving of access rights without undus deby in mg. Art, 21 Abs. 1 (e) (iii) RTS risk mg. 17.11 Ensum revelving of access rights without undus deby in mg. Art, 21 Abs. 1 (e) (iii) RTS risk mg. Ensum reverification of access rights at some accessing. Ensum reverification of access rights at some accessing.	management, mjelemented and verifield in a controlled manner. 18 de aufegand to preserve the availability, and a set of a set context of change management. 18 golg Encare a werflicktion that Life Caucity requirements have Art, 17 Abs. 2 (a) RTS risk	21:05 Have internat evaluation procedures to ICT-related and ICT-related Art. 17 Abs. 3 (e) DORA 21:06 International models in closent response procedures to operational models and evanues that envices become operational models accure in a timely manner. Art. 17 Abs. 3 (r) DORA 21:07 Here procedures and procedure to the model green on operational models and evanues. Art. 6 Abs. 2 (e) (R15 mix	contractual arrangement contractual arrangement and selection of subable (CT filmid, party service providers Ant. 28 Abs. 4(d) DORA Array and a selection of subable (CT filmid, party service providers services supporting critical or important functions services support device providers Arr. 4 Abs. 1 (d) RTB contractual arrangements contractual arrangements	24-07 fitting party services provider a solice frominant in the subcontracting 24-08 Perform inpact and searcements to essense the impact of a 24-08 Perform inpact and searcements for identification of risks 24-09 Perform inpact and the indext of the indext of a 24-09 Perform inpact and the indext of the indext of the indext of a 24-09 Performination and an association of insta 24-09 Performination and an association of insta 24-09 Performination and an association of insta 24-09 Performination and the indext of the ind	
	14-11 How socially measures to maune that thereworking and impact the C2 towards Art. 11 Abs. 2 (i) RTS inits impact the C2 towards How provident that non-production environments only that are an onymitted, passudoryminad or randomized and are an onymitted, passudoryminad or randomized interfaces and passing that are an onymitted or motion and the case of the case of the case of the case of the randomized or the case of the case of the case of the randomized or the case of the case of the case of the randomized or the case of the case of the case of the randomized or the case of the case of the case of the randomized or the case of the case of the case of the randomized or the case of the case of the case of the case of the randomized or the case of the case of the case of the case of the randomized or the case of the case of the case of the case of the randomized or the case of the case of the case of the case of the randomized or the case of the case of the case of the case of the randomized or the case of the case of the case of the case of the randomized or the case of the case of the case of the case of the randomized or the case of the case of the case of the case of the randomized or the case of the case of the case of the case of the randomized or the case of the case of the case of the case of the randomized or the case of the case of the case of the case of the randomized or the case of the case of the case of the case of the randomized or the case of	Ensumerecentification of access rights at least once a first give an all City stems and all steast every simulations; if City systems supporting critical or important functions; Assessments, analysis, supportacions & first humans 17:13 Perform site lassessments upon each major change in 17:14 Perform site lassessments upon each major change in 17:15 Perform site lassessments upon each major change in 17:16 Perform site lassessments upon each major change in 17:17 Performs the lassessments upon each major change in 17:18 Perform site lassessments upon each major change in 17:19 Perform site lassessments upon each major change in 17:19 Perform site lassessments upon each major change in 17:19 Performs the site lassessment exponents for changes to 11:10 Performance Performance 11:10 Performance 1	Assemmer; analysis, eporaches & instruments Assemmer; analysis, eporaches & instruments Performinida assessments upon each major change in Art. 8 Abs. 3 DORA Hore a tid, assessment approach for changes to Hore a tid, assessment approach for changes to Art. 9 Abs. 4 (e) DORA	Processes, plans, measures, protocols & tools 21 os 4see mechanisms to detect 1CT -related incidents, to 4see detection mechanisms to detect anomalous 4see detection mechanisms to detect 4see detection mechanisms 4see detection mechanisms 4see detection 4	23 Have a approvation process of new or methic changes to contract cual arrangements At Abs. 1 (0) RTS contract cual arrangements 23 Have a renewal process for contract cual arrangements At B. Abs. 4 RTS contract cual arrangements Assessments, onlyids, approaches & instruments Attemption	Ensure identification of LCI services supporting critical Art_4 empty RIS Monotinearting and under which of those are are provided in the area of the	
	Controllineary of state in the production terms on terms. 14.1 and the scheduling of production terms of CPT greaters among the CPT indication terms of the production terms of the terms of terms of the terms of ter	17:14 software, firmware components, systems or Art. 9 Abs. 4 (e) DORA Roles & Responsibilities Interponsibilities 17:15 New roles and responsibilities for granting: reviewing mg. Art. 21 Abs. 1 (e) (i) RTS/sisk mg.	In the security parameters Roles & Responsibilities Art. 17 Abs. 2 (b) RTS risk functions that approve charges and those responsible functions that approve charges and those responsible mgs.	Incidenta and potential material single points of failure To Hove advantatid subtrementary hashed on the second state of the s	Perform assessments for identifying whether contractual and the intermediate of ICF service supporting Ant. 28 Abs. 4 (a) DORA critical or important functions and the intermediate of th	Hore sestementation analyze the impact of material Art, 6 Abx, 1 BTS Subcontracting Art, 6 Abx, 1 BTS Subcontracting Art, 6 Abx, 1 BTS Subco	
	Ensure conducting of the development and testing in environments which are separated from the production Art. 2 Abs. 2 (b) (v) RTS risk mg. Assessments, subject, approaches & instruments 14-15 Contermon Cirk approaches & for for the production of the production T4-16 Ass. 2 (b) (v) RTS risk mg. Assessments, subject, approaches & instruments Assessments Assessments Art. 8 Abs. 2 DO RA	Report, Index, evidence & control Art. 20 Abs. 2 (b) RTS risk mpt, 17.10 Art. 20 Abs. 2 (c) RTS risk mpt, 17.17 17.10 Ensure review of identities and accounts mpt, 17.17 Art. 20 Abs. 2 (c) RTS risk mpt, 17.17	Here clear roles and responsibilities to the name that 1813 standard and responsibilities to the change and the times in an influence of the change and the times in an influence of the change and the times in an influence of the change and the times in an influence of the change and the times in an influence of the change and the times in an influence of the change and the times in an influence of the change and the times in an influence of the change and the times in an influence of the change and the times in an influence of the change and the times in an influence of the change and the times in an influence of the change and the times of the change and the times of the change and the	Here crisis communication plans enabling a responsible 21-12 circuitore d, et lesat, negli CT-related microinscriptor and the plans for communication test and the plans for communicati	Impact of the provision of CT anvices supporting critical crimparts functions by (17 thing party same) and (17 thing party same) and (17 thing party same) (17 thing party sam	24.13 reports on CT excuting of CD provided and reports on the social soci social social social social social social social social social	
	14.17 Perform CT firsk assessments before and Bitr concerning technologica splications or systems Art. 8 Ats. 7 D0 RA Reports, reviews, endonces & controls And the information needed to perform a first or the information needed to perform a Art. 4 Abs. 2(c) RTS risk mgt.	17.18 Here controls and tools to prevent unsultifortied access Art. 21 Alas. 1 (d) RTS risk to LCT asserts mg.	15:14 caster, sessence, sporzwal, implamented and verified in Art. 9 Abs. 4 (c) DORA 18:15 Ensure documentation and communication of change mgt. Aft. 17 Abs. 2 (d) RTS risk mgt.	Incidents 21-14 de ver elligiblion and monitoring measures for ICT-telated incidents Centre elligiblion and monitoring measures for ICT-telated centre information of clients about the measures that have been takento incident and about the measures takento incident and about takento	concentration ink concentration ink concentration ink concentration ink concentration ink concentration concentratin concentration concentration concentration concen	24.16 Here a documental CT Buckcentercling chain for OT Ar.5 Abs.1 BTS Buckcentercling Buckcentercling Buckcentercling Ensum monitoring of subcontracting conditions through review or contracts and documentation between CT. There's Ar.5 Abs.2 PSTS party service provides and subcontractions, and levy or dubcontracting Subcontracting advoctmantation between CT. There's Ar.5 Abs.2 PSTS advoctmantation between CT.	
	Here appropriate ICT solutions and poposesses that - ensure secure transfer data, - minimize the risk of comption or loss of data, unualificial access and licethical fallway that may approximate the solution of the solution of the solution of the 14-190 - sevenet the loss of any - ensure that data is protected from risks arising from - ensure that data is protected from risks arising from		Domain 19 IT project & project portfolio management	21:10 How mitigation and monitoring to ensure realiency against cyber threads Art. 6 Abs. 3 RIS risk mgt. 21:17 Have technical, cognitisational and operational mechanisms to support the CIT related incident pagement process including mechanisms to enable a prompt detection anomalous activities and behaviors Art. 22 Abs. 1 (c) RTS risk mgt. 14 Hew mechanisms to anomalous activities and behaviors To anomalous activities againfloat mechanisms for anomalous for activities againfloat mechanisms to anomalous for anomalous for activities againfloat mechanisms to anomalous for activities againfloat mechanisms for anomalous for activities again for anomalous for anomalous for activities and behaviors	23 19 Perform risk assessments to identify und relevant risks in Perform assessments to identify und analyze potential Perform assessments to identify und analyze potential Art. 28 Abs. 4(e) DORA Perform assessments whether and how subcontracting	24-18 Have documented subcontracts Art 5 Aler, 2 RTS Contextual requirements Subcontracting Value contractual signments ensuing a timely indication material requirements on the subcontracting Art 6 Aler, 1 RTS	
	-e-muse that data is protected form that a arring from the muse that the second seco		COBIT 19 TTL 4 ISO 2000 ISO 2700 BAD1: Managed Project management n/a A.6 Organization of Program Project management n/a A.6 Organization of Profession Portfolio management	21:10 related incidents and patterns mgt. Have tools generating alerts for anomalous activities affecting the completeness and the integrity of the data affecting the completeness and the integrity of the data Art. 23 Abs. 2 (b) RTS risk mgt.	23-21 Introductions and the sality for fully monitor the contractived supervise the financial entry in that respect. 23-22 Introductions and the sality for the complexity automotive by Art. 29Abs. 2 DORA Art. 5 Abs. 1 (a) (TS information Register Herein assessments of CT services related to information Register Herein assessments of an Abstract and alternatives Herein assessments of an Abstract of the continuity and alternatives Herein assessments to analyze whither the ICC third party	arrangements of the ICT third party service provider	
nce ations security	Physical and environmental security		DORArequirement DORArequirement Strategies, policies, frameworks, models & procedures	Ensure logging of anomatious activities in ICT systems 21:200 and network, including data and time of occurrence and Art. 23 Abs. 4 RTS risk mgt. detection, and the type of the anomatious activity. 21:21 Have classification ontended for ICT incidents Art. 3(c) RTS content of major incident reports Assessments, analysis, approaches & instruments When excerning from and IC-related incident, perform	23.23 bervice provide that sufficient resources to ensure that Ar. J Aba. 6 RTS contractual anargement with all is togat and anargement and	ICT provider & service level management	
	DSSS: Hanaged Information security n/o A-11 Physical and security Services Information security n/o Revisionmental security Information of the security of the security of the security DORA requirement DORA requirements		19:01 Have a documented IC Tproject management policy Ar. 15 Abs. 1 RTS risk mgt. Assessments enalysis, sponcaches & instruments Instruments 19:02 PerformCIP project risk assessments Art. 15 Abs. 3 (d) RTS risk mgt. Roles & Responsibilities Instruments Instruments	21:22 excessing vice-loss in order to ensure that the highest consistent tetrement systems. Art. 12 Abs. 7 DORA Have assessments to analyze the potentialingsct of videnebilities and optent threats, Cl ⁻¹ ratisted incidents, including optent threats, Cl ⁻¹ ratisted incidents, and the potentialities and optent threats, Cl ⁻¹ ratisted incidents, and the potentialities and optent threats, Cl ⁻¹ ratisted incidents, and the potentialities and the potential tetra and the potentialities and and the potentialities and the potentialities and the potentialities and and the potentialities and the potentialities and the potentialities and and the potentialities and the potentialities and the potentialities and and the potentialities and the potentialities and the potentialities and and the potentialities and the potentialities and the potentialities and and the potentialities and the potentialities and the potentialities and and the potentialities and the potentialities and the potentialities and and the potentis and the potentis and the potentis and and the potential	23 25 Ensure identification of the branches of francial entities A. SAbs. 1 (c) ITS 23 25 Ensure identification of the ICT third party service Information Englisher 23 26 Ensure identification of the ICT third party service Information Englisher 23 26 Ensure identification of the ICT third party service Information Englisher 23 27 Ensure identification of the entities regime the model and englisher information Register 23 27 Ensure identification of the entities regime the information Register	APO10 Managed Suppler management 8.3.4 Suppler management Vendors Suppler management APO09 Managed Service level 8.3.3 Service level Service Agreements management APO11: Managed Continual Improvement Coll Service Agreements Apont Apon	
भ भ	Strategies, policies, finanzemotia, modela & goucaduras 15:01 reprincipante interficiente physical access of deformation assess and CCT parents to achesia requires (resp. 14, 9, 40, 9,		19:03 Have notes and responsibilities for ICT projects Art. 15 Abs. 3 (b) RTS risk mg. Report, mixing, enderses & controls Image: Control of the second seco	21:24 Perform forensic analysis for ICT-related incidents, where necessary mappinde and evolution of ICT related incidents, in particular optimum and their patterns, while we 21:25 Art. 13 Abs. 2 (b) DORA 21:24 Internet incidents, in particular optimum and their patterns, while we subsetstanting the level of ICT risk separare, in particular in relation to relation or total or in prostantinuctions, Art. 13 Abs. 4 DORA	Yates a methodology and perform assessments to the sector of the sector assessments to functions Art. 3 Abs. 3 RTS contractual anangements 23.29 envices supporting critical or importent touristics Art. 3 Abs. 3 RTS contractual anangements 23.29 envices supporting critical or importent the ad aligner process Art. 3 Abs. 3 RTS contractual anangements	Ouslay Continual Improvement DORA requirement DORA requirement Strategies policies, frameworks, models & procedures	
LPT	15:00 Issues a bate data pairing for pagera wand data software (of periodramodor sociality facilities) neg. (1 + 18 Abs. 2 (e) RTS nisk neg. (2 + 10 + 10 + 10 + 10 + 10 + 10 + 10 + 1		Domain 20	and enhance the cyber maturity and preparedness of the framacial enhance. 21.26. dft/cflandstring/stand 21.27. Have early warning indicators for/Cfl related incidents 21.27. Have early warning indicators for/Cf related incidents 21.27. Have early warning indicators for/Cf related incidents	Perform assessments on the existence of risk mitigation 23.30 and unlinears continuing reasons within the ICT time. Party service provider Role & Rocanobilities Have a control function to provide the control tube.	Hore a documental policy on the use (ICI privides 2501 supporting entities of important functions provided by ICI third party service providers Art. 4 Abs. 1 RTS contractual anangements Processes, plan, measure, protocols & tools Ensure including ICI third and service convides	
LPT	hazardá 15 05 Have mesuses to secure ICT assets, both within and Mrt. 18 Abs. 2 (c) RTS risk mgl. 15 05 Have mesuses to provide appropriate protection to Mrt. 18 Abs. 2 (c) RTS risk mgl. 15 06 Have mesuses to provide appropriate protection to Mrt. 18 Abs. 2 (c) RTS risk mgl.		Acquisition, development and maintenance of ICT systems and EUA/IDP	21:38 Here assessments of possible cross-border impacts of Art. 19 Abs. 1 DORA 21:39 Here assessments to analyze significant or recurring Art. 2 Abs. 1 (e) RTS risk recommon of C1 Andred Folders. 21:30 Cross of C1 Andred Folders. 21:30 Cross of C1 Andred Folders.	23 31 agreements with third party service providers, the ICT ICT third party risks Art. 5 Abx. 3 DORA 23 32 Encode provided under these arrangements and reliable ICT third party risks Art. 1 Abs. 2 (9 (i) 815 esk mgt. 23 32 Encode battlese the financial entity and the ICT exponsibilities battlese the financial entity and the ICT and your service provides Art. 1 Abs. 2 (9 (i) 815 esk mgt. 23 33 Have audites conducting impercitoris and audits on ICT Art. 28 Abs. 6 DORA Art. 28 Abs. 6 DORA	constraint at reliance training, where asymptotiate 25 G3 the technical and organisational measures to minimize the rink and startice do the infrastructure usedby the rink and startice overlaw from the Characteria startic considering leading practices and attracted Hayes corceases for each infrast holds of the Nevula of	L
LPT	Have measures the ensure the variability, submitricity, and physical access control devices Art. 18 Abs. 2(d) RTS risk mgt. 15:007 and physical access control devices Have subgraduated to preserve the availability, accentered up, height and confidentiatility of data in content of physical security Art. 18 Abs. 1 RTS risk mgt. 15:003 accented of physical security Art. 18 Abs. 1 RTS risk		AP-008: Managed Relationships Release management deprogram deproved deprove	24132 Construction of information 21.33 Construction of information 21.34 Construction of information 21.32 Abs. 2 (d) RTS risk mgb, 21.32 Abs. 2 (d) RTS risk risk 21.32 Abs. 2 (d) RTS risk 21.32 Abs. 2 (d) RTS risk	2-33 third party services providers All. Service. Service Report, eventy eventy eventy All. Service. Service All. Service. Service 2-3.4 Strater sporting on the number of new contractual All. 28 Abs. 3D DRA 2-3.35 Strater sporting of all data points in the register of Register All. 4 Abs. 313 information Register	25-04 the use of CT anxies provided by CT thirdy party Art. 4 Abt. This commental amongments Have measures to monitor compliance with requirements regarding the confidentially, validability the dy by plance of the ICT thirdy party privice private with the financial tertity interest policies and amongments	
i risk	15:07 Have physical access control measures Aff. 21 Add. 1 (g) ht 5 miles		Bokulons likentification and the string management APO11: Managed Quality Deployment management Continual improvement Petationalp	21-33 decomprise and other ICT-restendent concident and Mr. 4. 4. RTS ACT incidents Member Status, and and an an and an an and an an and an and an and an and an and an	23 36 Ensure review of the policy on the use of CT anvices Art. 5 Ats. 2 (h) DORA 23 37 Ensure review of CT find darty risk strategy Art. 28 Ats. 2 DORA 23 38 Ensure review of CT find darty risk strategy Art. 28 Ats. 2 DORA	procedures. 25 06 large measures to adopt if shortcomings of the ICT third- party service provider are identified Assessments analysis, exponders & instruments Assessments in anylis, exponders & instruments and the instruments and the instruments and the instruments are assessments to maintain the instrument and the instruments are assessments to maintain the instrument and the instruments are assessments to maintain the instrument and the instruments are assessments to maintain the instrument and the instruments are assessments to maintain the instrument and the instruments are assessments to maintain the instrument and the instruments are assessments to maintain the instrument and the instruments are assessments are assess	
LPT	Vulnerability & patch management COBIT 19 ITL 4 ISO 2000 ISO 27000 DSS05: Managed Information security na A:12 Operations security		management Business analysis DORA requirement DORA refuterence	Have assessments to analyze whether the incident 21-33 disciplication of that are supervised by authorization, registration of that are supervised by authorization, registration of that are supervised by 21-36 Art. 6 (b) RTS ICT incidents 21-36 disciplication of the intervised and the the incidents approximation of the intervised and the the incident of approximation of the intervised and the intervised and supervised and constraints the incident of the incidents Art. 6 (c) RTS ICT incidents	2.39 Ensure review of NDA Aff. FARE. 1(c) https://mg. 23.40 Ensure review of information register Art.3 Abs. 21TS information Register 23.41 Ensure review of adsessment to determine CT services Art.3 Abs. 21TS contractual anragement functions 23.41 Ensure review of adsessment to determine CT services Art.4 Abs. 1(c) RTS 24.41 Ensure review of information functions Art.4 Abs. 1(c) RTS	25 07 requirements to maintain digital operational realisione provides Art.1 Abs.2 (b) RTS risk mgt. 25 08 to seast or services operated by/CT third pary provides Art.9 Abs.1 RTS contractual arrangements 25 08 Have measures and key indicators to montor and assess the performance of CTT hird pary service arrangements Art.9 Abs.1 RTS contractual arrangements	
STLPT	Security Services management in cyclestaria security DORA requirement Company DORA requirement Strategies, policies, ferneworks, models & procedures		Strategies, policies, frameworks, models & procedures 20 01 Have a documented policy gaverning the acquisition, development and maintenance of ICD systems Art. 16 Abs. 1 RTS risk mgt. 20 02 Have a documented to policy gaverning the acquisition, development and maintenance procedure Art. 16 Abs. 2 RTS risk mgt. 20 03 Have acquisition, development and maintenance procedure Art. 16 Abs. 2 RTS risk mgt.	financial entity, 137 days an impact assessment for classification of CT 141.9 Abs. 1 (I) RTSICT incidents 21.33 days assessments to unalyze the economic impact of ECT-related incidents ECT-related incidents 15.15.45.25.07.07 ECT-related incidents 15.15.45.25.07.07	23.42 use of CT annovas supporting citical or important A.4 Abs. 1 (c) (RTS control in the support of the support	Improvides Art. 9 Atta: 2 RTS contractual performance of CT services provided (), CT find party amagements Art. 9 Atta: 2 RTS contractual amagements Interview provides Interview provides Art. 9 Atta: 2 RTS contractual amagements Interview provides Interview provides Art. 9 Atta: 2 RTS contractual amagements Interview provides Interview provides Art. 9 Atta: 2 RTS contractual amagements Interview provides Interview provides Art. 9 Atta: 2 RTS contractual amagements	
PT T	16:01 Have documented policies for patches and updates Art. 5 Ats. 4(f) DDRA Have documented vulnesability management procedures No works ensuing the exciting of the those adjusted at the exciting of the those adjusted at the exciting of the those adjusted at the excitation of the those adjusted at the those adjusted		Ensure consideration and implementation of ICT 20 03 systemance to ICT systems developed or managed by users outside the ICT function, Here policies and procedures to manage the ICT operations of ICT assets with a view to ensure the	Holdertis on a monthly basis How assessments to availage whether the cyber that could affect or could have affected or ling or the cyber that could affect or could have affected or ling or the cyber that financial entities, third party providers, clients or financial counterparts	Contractual requirements Have documented contractual agreements with ICT 23.46 Have documented contractual agreements with ICT DORA.rt. 1 Abs. 1(b) DORA	Indepandent reviews Report, without a schortish Z5 12 Asse reports of ICT third party service provide on Art. 30 Abs. 3(b) OCRA Art. 70 Abs. 2(c) NTS disk regulation actions Art. 30 Abs. 3(b) Abs. 3(c) Abs.	
T	Have procedures for disclosure of victorenabilities to Ho 30 = 10 = 20 = 20 = 20 = 20 = 20 = 20 = 2		20.04 security of retrotions, enabling sidesparse sarbigiants and the intraviours and other services and proceedures data as part of the CT ancurby policies and procedures Processes, beam near-serve, policies and procedures and the service of the service and the service of th	21:41 Have assessment to analyze whether the cyber threat Ar. 13 Abs. 1 (b) RTS/CT Perform a rekennet autorities in other Incidents Incidents 21:42 Execution is invested for competent autorities in other Ar. 13 enaph RTS/CT Perform a rekennet based Execution is in other Ar. 13 enaph RTS/CT Perform a rekennet based Execution is in other Ar. 13 enaph RTS/CT Perform a rekennet based Execution is in other Ar. 13 enaph RTS/CT	Have documented confidentiality or non-disclosure At 1.4 Abs. 1 (c) RTS risk mg. 23.47 mg. At 1.4 Abs. 1 (c) RTS risk mg. 23.48 Masue of distribut contractual chases developed by public authorities for specific services Art. 30 Abs. 4 DORA 23.49 Have a documented planned timeline for implementation. Art. 30 Abs. 4 DORA 23.49 Have a documented planned timeline for implementation. Art. 30 Abs. 4 DORA	Anno privide Colometra provide particle delivery agente Software provides and the colometra provide delivery agente Software provides Anno 2012 Software and testing of CT third party service provides Anno colometra of CT third party service provides Software colometra of CT third party service provides Anno colometra of CT third party service provides Anno colometra of CT third party service provides	
STLPT	eonfetentially of data 16.05 Hope emergency procedures for the patching and Job Hope excelution procedures for the patching and In the excelution procedures in case the deaders for the indication of offshore and hardware patches and In the excelution processing of the excelution of the excelution of the Interview of the excelution of the excelution of the excelution of the Interview of the excelution of the excelution of the excelution of the Interview of the excelution of the excelution of the excelution of the Interview of the excelution of the excelution of the excelution of the excelution of the Interview of the excelution of the excelution of the excelution of the excelution of the Interview of the excelution of the excelution of the excelution of the excelution of the Interview of the excelution of the exceluti		terrs antigisation to prenerre the periability, terrs antigisation to prenerre the periability, terrs and the p	Have a role ensuing the implementation of the 1214 click Art. 14 Abs. 3 DORA Art. 14 Abs. 3 DORA Milling the public and media function for that purpose. 21-44 add media function for that purpose. Art. 17 Abs. 3 (c) DORA Art. 17 Abs. 3 (c) DORA Have roles and responsibilities to effectively detect and Have roles and responsibilities to effectively detect and Art. 17 Abs. 3 (c) DORA	Have audit arrangements on information access, agreements Art. BAbs. 1 (g) RTS agreements 23 51 Review compliance of DT third party service providers with most up-badte and highest quality information with most up-badte and highest quality information Art. 28 Abs. 5 DORA	Scorey payment reason accession of the second	
PT	Processes, plans, measure, protocols & tools 16:07 Resins and possible updates of the tools Art. 10 Abs. 2 (d) RTS inits and UB service of the tools of tools of the tools of tools of the tools of tools of the tools of tools of the tools of tools of the tools of the tools of tools		systems systems important Bystems orgen deteration or interlates the risk of unintensional alteration or interlates the risk of unintensional analyzes and adaptives and	activites. Reporting, wirking, wirking as & controls Reporting of major ICT related incidents to the Competent automities Forum expecting of major ICT related incidents to the Evenue reporting of major ICT related incidents Forum expecting of major ICT related Forum expec	Register, liberies, invertories Att. 28 Abs. 3 DORA 23 52 Have a documented register of information Art. 28 Abs. 3 DORA	25-17 revise service provides	
_	by the financial entity itself or customized or developed by CT that party services provider. 16 07 Have action parts to address witherabilities and Assessments, analysis, approaches & instruments		20-10 Have action pixe to address vulnerabilities and macratiles in source code Art. 16 Abs. 2 (b) RTS risk mgt. 20-11 Performs source code reviews covering both static and dynamic testing Art. 16 Abs. 2 (b) RTS risk mgt. 21-22 Covering to the source code reviews covering both static and dynamic testing Art. 16 Abs. 2 (b) RTS risk mgt.	21-47 payment-related incidents to the competent authonities Art. 1 Abs. 1 (a) (a) DORA Ensure reporting of aggingated annual cost and losses authonities Art. 1 Abs. 1 (b) (a) DORA 21-49 caused ymaint/Clrevisted incidents to the competent authonities Art. 1 Abs. 1 (b) (DORA 21-49 Have CL7-related incidents reports Art. 6 Abs. 8 (f) DORA 21-50 Have ECT-related incidents Art. 7 Abs. 2 DORA			
security	How an assessment of opter threats and ICT Art. 8 Abs, 2 DORA 16-10 International selection with the ICT supported business functions, information assets and ICT axets Art. 8 Abs, 2 DORA 16-10 vulnerabilities relevant threats, ICT related incidents, incidence and cyber threats, ICT related incidents, resilience Art. 13 Abs, 1 DORA Ensure identification and update of information Art. 10 Abs, 2 Ab IST side		Assessments, analysis, approaches & instruments Ensure identification of tachinal specification and ICT acquaistion, development and maintenance of ICT acquaistion, development and maintenance of ICT servers	Hore a list of contacts with internal functions and and the address of t			
	16-12 Perform automatic management of montaneous Art. 17 Abs. 2 (a) ATS risk mgt. 16-13 Perform automatic valuerabilitys, consing and assemrate and the second and and and and and and and and and mgt. Art. 10 Abs. 2 (b) ATS risk mgt. 16-14 Emanue isoenficiacion of ontente to privinitize the assemrate and Testing and thermitigation measures mgt. Art. 10 Abs. 2 (b) ATS risk mgt.		20-14 Ensure identification and analysis of vulnerabilities and somalies in source code Int EAbs. 2(t) RTS risk mgt. Have assessments to analyze proprietary software and source code prior to their deployment in the production environment. An. 16 Abs. 2(t) RTS risk mgt. Reports, mview, evidences & controls Environment.	21:53 Have a classification of LCT incidents Af. 22 Ass. 1 (d) RTS risk mgt. 21:54 Have a classification of LCT incidents mgt. 21:54 Have a clossification of LCT incidents mgt. 21:55 Have a clossification of LCT incidents mgt. 21:50 Have a clossification of LCT incidents mgt. 21:50 Incident report. This incident reporting Art. 1 SAbs. 1 20:52 Doppring Art. 19 Abs. 1 DOpRing.			
mgt.	Ensure identification and evaluation of available 16-15 admine and hardware patches and updates by using automated tools, where possible 16-16 Ensure identification and nanysize of vulnerabilities and Finandes in source code Market and State (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		20.1 Specification earls (T) carbonical maintenance of (CT) systems, Art. 16 Abs. 1 (b) RTS risk maintenance of (CT) systems, 20.1 Have controls to protect the integrity of the source code Art. 16 Abs. 2 (c) RTS risk mgl. Art. 16 Abs. 2 (c) RTS risk mgl. 20.1 Monitor the imgementation of action plans to address this is the source code mgl. Art. 16 Abs. 2 (c) RTS risk mgl.	Competent autorities DORA 21:56 Encoded to addet reviews and detertification of required improvements to the ICT operations Art.13 Abs. 2DORA			
mgt. sk sk	16-17 Second provide population of the production of the produ			Domain 22 Monitoring, Availability, Capacity & Performance Management			
Srisk Srisk 'Srisk	16-19 Entrate monitoring and very the remeatation of mgL APL 1/VABL 4 (g) in 1 mix mgL 16-30 Have records of detected vulnerabilities affecting (CT mgL AT 10 Abs. 2 (h) RTS init mgL 16-31 Monitor the implementation of action plants to address APL AT, 16 Abs. 2 (h) RTS init mgL 16-32 Perform source code reviews covering both static and the administer interplant of the implementation mgL AT, 16 Abs. 2 (h) RTS init mgL			COBIT 19 ITIL 4 ISO 20000 ISO 27000 DSS01: Managed Operations Monitoring and event management 9.1 Monitoring, measurement, and your, A.12 Operations security and evaluation Measurement and responing Measurement and responing Measurement and responing			
"Srisk Srisk sk	16-22 dynamic testing mgt. 16-23 Ensure security testing of software packages Art. 16 Abs. 2 (b) RTS risk mgt.			OORArequirement Exemplary DORArelevance Strategies, policies, frameworks, models & procedures			
sk 3 risk 6 risk				Have documented capacity and performance Art. 9 Atts. 1 RTS risk mgt. 22 01 magnetic procedures to identify capacity and performance 22 01 magnetic procedures identify capacity and monitoring procedures to maintain and minitoring vid data and ICT general mean and Hicinicary of U systems and pervent ICT systems and ICT syst			
				the ICT operations of ICT assets with a view to ensuring			

Note decumented policies and procedures to manage the CT operation of ICT sates shall a version ansuing against intrustron of ICT sates shall be version ansuing against intrustrons and data masses and proceedings without the CT security policies indertainsity of data as part of the CT security policies and procedures

 22:04
 Have policies and procedures for ICT operations including controls and monitoring of ICT systems
 Art. 8 Abs. 2 (b) RTS risk mgt.

 24:05
 Have policies and procedures to manage the ICT operations of ICT assets as part of the ICT security policies and procedures
 Art. 8 Abs. 2 RTS Risk Management

22-06 Have policies and procedures for ICT operations including controls and monitoring of ICT systems Management

Processe, plan. messures, protocol & tool
 Aver redunders (D' capacities (e.g. a secondary
 processing site equipped with excurse, capabilities
 and functions that are adequate to ensure business
 needs.

Heeks
 Heve appropriate measures to cater for the specificities
 dirlCT systems with long or complex procurementor
 approval processes of that are source-intensive
 Report, where, enklances & controls
 Monitor and control:the security and functioning of ICT
 Art. 9 Abs. 2 ATS frisk mgt.
 Att. 9 Abs. 2 A

© Copyright 2024 | Dr. Marlen Hofmann | Alle Inhalte, Insbesondere Texte, Fotografien und Grafiken sind urbe

BAIT 10 (MaRisk AT 9)

(IT) Notfallmanagement

Domain 26 ICT business continuity management

APOII: C	Managed Service continuity and 2 innuity Continual improvement Continual improvement Continual improvement Continual improvement Continual improvement Continual improvement Continuation Conti	y policy as y rocedures and anagement twes reentiating and methods and methods and data with loss entation of issue that staff, ICT rentation of issue that staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant sup	nur 21 Alformator security supparts of business continuity management DORA Reference Art. 5Abs. 2 (e) DORA Art. 11 Abs. 2 DORA Art. 11 Abs. 2 DORA Art. 12 Abs. 1 (e) DORA Art. 2 Abs. 2 (e) DORA Art. 14 Abs. 2 DORA
# Strategie 26-01 26-02 26-03 26-04 26-05 26-05 26-06 26-07 26-08 26-09 26-09 26-09 26-09 26-09	DORA requirement a policies Internetos model de Sarcodo Nera documente la Chaniera contraina policies Internetos de La Chaniera contraina policies de la contrate la Chaniera contraina tivo esta ducimiente de la Chaniera contraina la contrata de la Chaniera contraina y la vera de actimiente de la Chaniera particular la staff responsible for response particular la staff responsible for response and la contrata de la contrata de la contrata la staff response and response la staff response and response la staff response and response particular staff response and response la staff response and response and response activitation parte enabilità de la staff response and response la staff contrata de la contrata de la Staff staff response and response and response activitation parte enabilità de la staff response and response la staff contrata de la contrata de la Staff staff contrata de la staff contrata de l	y policy as y rocedures and anagement twes reentiating and methods and methods and data with loss entation of issue that staff, ICT rentation of issue that staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant sup	Reference Art. 5Abs. 2(e) DORA Art. 11 Abs. 2006A Art. 11 Abs. 2006A Art. 12 Abs. 5 (b) DORA Art. 12 Abs. 1 (b) DORA Art. 12 Abs. 1 (b) DORA Art. 24 Abs. 1 (b) RT5 mik mg. Art. 5Abs. 2 (e) DORA Art. 5Abs. 2 (e) DORA
Strategie 226-01 226-02 226-03 226-04 226-05 226-05 226-06 226-07 Processor 226-08 226-09 226-09 226-09	a policies, frameworka, models & procedi Ware as documented. ET business continuity oper- and of the overal business continuity oper- tances of the overal business of the overall business processing of the overall business of the overall business and business of the overall business of the business of the overall business of the overall the overall business of the overall business of the business of the overall business of the overall business of the overall business of the overall business of the business of the overall business of the overall business of the business of the overall business of the overall business of the business of the overall business of the overall business of the business of the overall business of the overall business of the business of the overall business of the overall business of the business of the overall business of the overall business of the business of the overall business of the overall business of the business of the overall business of the overall business of the business of the overall business of the ov	y policy as y rocedures and anagement twes reentiating and methods and methods and data with loss entation of issue that staff, ICT rentation of issue that staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant sup	Reference Art. 5Abs. 2(e) DORA Art. 11 Abs. 2006A Art. 11 Abs. 2006A Art. 12 Abs. 5 (b) DORA Art. 12 Abs. 1 (b) DORA Art. 12 Abs. 1 (b) DORA Art. 24 Abs. 1 (b) RT5 mik mg. Art. 5Abs. 2 (e) DORA Art. 5Abs. 2 (e) DORA
26-01 26-02 26-03 26-04 26-04 26-05 26-05 26-05 26-07 26-08 26-09 26-09	Here a documented D Taurises contributions and the overall business contribution years represent the contract business contribution years representations of the transmission of the sec- temportal sectors of the sector of the sec- temportal sectors of the sector of the sec- sion of the sectors of the sector of the sec- sent sectors of the sector of the sector of the sec- sent sectors of the sectors of the sectors of the sec- sent sectors of the sectors of the sectors of the sec- tor sectors of the sectors of the sectors of the sec- tor sectors of the sectors of the sectors of the sec- tor sectors of the sectors of the sectors of the sec- tor sectors of the sectors of the sectors of the sec- tor sectors of the sectors of the sectors of the sectors of the sectors of the sectors of the sectors of the sec- tor sectors of the sectors of the sectors of the sec- tor sectors of the sectors of the sectors of the sec- tor sectors of the sectors of the sectors of the sec- tor sectors of the sectors of the sectors of the sec- tors of the sectors of the sectors of the sectors of the sectors of the sectors of the sectors of the sec- tors of the sectors of the sectors of the sectors of the sectors of the sectors of the sectors of the sectors of the sectors of the sectors of the sectors of the sectors of the sectors of the sector of the sectors of the sectors of the sectors of the sectors of the sectors of the sectors of the peak of the sectors of the se	y policy as y rocedures and anagement twes reentiating and methods and methods and data with loss entation of issue that staff, ICT rentation of issue that staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant staff, ICT superstant sup	Art: 11 Abs; 2008A Art: 12 Abs; 5 (b) DORA Art: 14 Abs; 2008A Art: 14 Abs; 2008A Art: 24 Abs; 1 (b) DORA Art: 24 Abs; 2 (c) RT5 mk mg; Art: 5 Abs; 2 (c) DORA
26-02 26-03 26-04 26-05 26-05 26-07 26-07 26-08 26-09 26-09	Here documented anagements, plans, p mechanismi effo "Louismes continuity me have defined accever (time & point) object to the second second second second second best of the second second second second best of the second second second second best of the second second second second second second second second second second second second second second second second for manufacture the affect second s	rocedures and anagement trèss arentiating lennt, in and methods and methods and methods and data with loss ventation of sure that staff, ICT s rey plans a responsible cidents or s s well as to	Art: 11 Abs; 2008A Art: 12 Abs; 5 (b) DORA Art: 14 Abs; 2008A Art: 14 Abs; 2008A Art: 24 Abs; 1 (b) DORA Art: 24 Abs; 2 (c) RT5 mk mg; Art: 5 Abs; 2 (c) DORA
26-03 1 26-04 2 26-05 2 26-06 2 26-07 2 26-08 2 26-09 2 26-09 2	Here defined recovery (time & paint) object Here communication policies to suff offer particular the safet reported by the safet of the particular the safet reported by the safet of the the retrotation and saff that needs to be informed Have retrotation and concervation of CPT systems and information and worthing the retrotation of CPT systems of the safet of the saf	tives sentiating sent, in and methods and data with loss wentation of sure that constraints are that constraints are sponsible idents or se well as to file.	Art. 12 Abs. 5 (b) DORA Art. 14 Abs. 2 DORA Art. 14 Abs. 2 DORA Art. 12 Abs. 1 (b) DORA Art. 24 Abs. 1 (c) RTS risk mgt. Art. 25 Abs. 2 (c) DORA
26-04 26-05 26-06 26-07 26-08 26-09	Here communication policies for shall offer between shalf involved in CTr iak managem particular the shaft responsible for mapping and the shaft responsible for mapping the set statistic shaft and the source proceedures a share set statistic shaft and source proceedures a involved the set of the	erentiating erent, in and ad and methods and data with fuloss sure that staff, ICT is ery plans a responsible idents or s s well as to	Art. 14 Abs. 2 DORA Art. 12 Abs. 1 (b) DORA Art. 24 Abs. 1 (c) RTS risk mg. Art. 25 Abs. 2 (c) RTS risk mg. Art. 5 Abs. 2 (c) DORA
26-06 26-07 26-08 26-09 26-09	Neve exclusion procedures for the implem the CT business control by the observation of the building of the second second second second second the control of the second se	entation of isure that staff, ICT ind ICT is ery plans ta responsible cidents or as well as to	Art. 24 Abs. 1 (e) RTS risk mgt. Art. 25 Abs. 2 (e) RTS risk mgt. Art. 5 Abs. 2 (e) DORA
26-07 Processes 26-08 26-09	Here proceedures to well, the ability of the the here proceedures to well, the ability of the this party and/or services. If O yearns a services to respond adequately to scenario and the documented for the gools and these documented for the gools and these documented for the gools and the public, as appropriate methodocument of the analysis. The the public, as appropriate methodocument of the analysis of the public, as appropriate methodocument of the analysis of the methodocument o	staff, ICT ind ICT is ery plans a responsible cidents or iss well as to	mgt. Art. 25 Abs. 2 (e) RTS risk mgt. Art. 5 Abs. 2 (e) DORA
Processer 26-08 26-09	s, plans, measures, protocols & tools Have documented ICI response and recover taring into account the results of the BIA Have crisis communication plans enabling disclosure of, st least, majorICI-related in vulnerabilities to clenst and counterparts the public, as appropriate Have plans with containment measures, pr technologies suited to each type of ICI relations and ICI relations and ICI relations and ICI relations and the relation of ICI relations and ICI relations and accounterparts and the relations of ICI relations and accounterparts and accounterparts and the relations and accounterparts and the relation of the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation of the relation accounterparts and the relation of the relation o	ery plans a responsible cidents or as well as to	mgt. Art. 5 Abs. 2 (e) DORA
26-08	s, plans, measures, protocols & tools Have documented ICI response and recover taring into account the results of the BIA Have crisis communication plans enabling disclosure of, st least, majorICI-related in vulnerabilities to clenst and counterparts the public, as appropriate Have plans with containment measures, pr technologies suited to each type of ICI relations and ICI relations and ICI relations and ICI relations and the relation of ICI relations and ICI relations and accounterparts and the relations of ICI relations and accounterparts and accounterparts and the relations and accounterparts and the relation of the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation accounterparts and the relation of the relation of the relation of the relation accounterparts and the relation of the relation o	ery plans a responsible cidents or as well as to	
26-09	Have crisis communication plans enabling disclosure of, at least, major ICT-related in vulnerabilities to clients and counterparts a the public, as appropriate Have plans with containment measures, pr technologies suited to each type of ICT-related removable of kinet of enarch type of ICT-related and the submet of enarch type of ICT-related technologies suited to each type of ICT-related technologies suited technologies suited to each type of ICT-related technologies suited technologies suited technologies t	a responsible cidents or as well as to	
26-10	Have plans with containment measures, pr technologies suited to each type of ICT-rela	a responsible cidents or as well as to rocesses and ated incident	Art. 14 Abs. 1 DORA
26-10	Have plans with containment measures, pr technologies suited to each type of ICT-rela	rocesses and sted incident	
	Have ICT business continuity plans and ens		Art. 11 Abs, 2 (c) DORA
26-11	contracted ICT services relevant for critical functions	sure their urced or l or important	Art. 11 Abs. 4 DORA
Assessme	ents, analysis, approaches & instruments		
26-12	Ensure risk assessment of challenges facer activation of ICT business continuity plans a response and recovery plans	d upon the and ICT	Art. 13 Abs. 3 DORA
26-13	mave a business impact analysis to assess impact of severe business disruptions	the potential	Art. 24 Abs. 1 (a) RTS risk mgt.
26-14	Ensure identification of relevant scenarios f response and recovery plans, taking into ac- following scenarios: 1] cyber-takcks and as failures of ICT third-party service provider.3 failures of ICT third-party service provider.3 premises, 4] failures of ICT assets or commu- infrastructure:5] non-valiability of staft, 6] honge, natural ideasters, pandemic, and p statacks, 8] political and service natability.3] widespread power outgase	witchovers 2) 3) failure of unication	Art. 11 Abs. 6 DORA
26-15	Ensure documentation and analysis of test business continuity tests	results of	Art. 25 Abs. 5 RTS risk mgt.
26-16	Ensure that ICT response and recovery plan of internal audit reviews	ns are subject	Art. 11 Abs. 3 DORA
26-17	Asponsibilities Have a control function to oversee the imple ICT business continuity policy and ICT respo recovery plans	ementation of onse and	Art. 5 Abs. 2 (e) DORA
26-18	Have a crisis management function to set o procedures to manage internal and externa communications in the event of activation or business continuity plans or ICT response a plans	out Il crisis of their ICT and recovery	Art. 11 Abs. 7 DORA
26-19	Have roles and responsibilities to implement business continuity policy	nt the ICT	Art. 24 Abs. 1 (e) RTS risk mgt.
Reports, r	raviews, evidences & controls		
26-20	Have management reports on identified det context of business continuity tests	ficiencies in	Art. 25 Abs. 5 RTS risk mgt.
26-21	Ensure review of ICT business continuity po ICT response and recovery plans	ouy and of	Art. 11 Abs. 6 DORA Art. 24 Abs. 1 (i) RTS risk
	Ensure review of the effectiveness of ICT bu continuity plans Test the ICT business continuity plans and t		Art. 11 Abs. 6 (b) DORA
	response and recovery plans Test the crisis communication plans		Art. 11 Abs. 6 (b) DORA Art. 11 Abs. 6 (b) DORA
26-25	Have records of activities before and during events when their ICT business continuity p response and recovery plans are activated	g disruption alans and ICT	Art. 11 Abs. 8 DORA
26-26	Ensure testing of ICT business continuity pla third-party service providers	ansofICT	Art. 30 Abs. 3 (c) DORA
	Ensure testing of ICT services provided by IC service providers		Art. 25 Abs. 2 (b) RTS risk mgt.
26-28 i	Perform testings of ICT business continuity assess the ability to ensure the continuity o important functions	plans to of critical or	Art. 25 Abs. 2 RTS risk mgt.
Contractu	ual requirements Have documented ICT business continuity a with ICT third-party service providers		Art. 11 Abs. 4 DORA
	with ICT third-party service providers Have ICT business continuity plans and ens maintenance and testing notably for outsou contracted ICT services relevant for critical functions		Art. 11 Abs. 4 DORA
	functions Have contingency measures to maintain bu continuity in the event of business disruptio inappropriate or failed provision of ICT servi		Art. 26 Abs. 4 RTS Risk Management