algosec

Secure application connectivity. Anywhere.

DORA compliance with AlgoSec

The Digital Operational Resilience Act (DORA) mandates that financial institutions maintain resilient IT and network systems to mitigate risks like cyber threats and operational disruptions. Starting in early 2025, organizations must align their network security and compliance strategies with DORA's requirements, which emphasize operational resilience, data protection, and continuous compliance.

AlgoSec, a leader in network security policy management, enables financial institutions to navigate DORA's regulatory landscape effectively. This solution brief explains how AlgoSec's application-centric approach, automated processes, and enhanced visibility help streamline compliance efforts, improve security posture, and ensure operational resilience.

Key challenges addressed by DORA

Operational resilience

Financial institutions must ensure their IT and network operations remain resilient against cyberattacks and disruptions. DORA requires companies to detect, respond to, and recover quickly from incidents.

Network and data security

With increasingly complex digital infrastructures, safeguarding sensitive data and ensuring network security are top priorities. DORA emphasizes the need to mitigate cyber risks while maintaining the resilience of critical applications.

Compliance and reporting

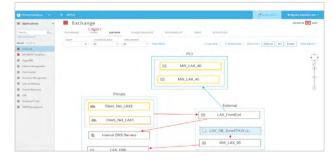
Continuous monitoring and detailed reporting are essential for staying compliant with DORA. Traditional, manual approaches to compliance are no longer sufficient, as they are time-consuming and error-prone.

How AlgoSec supports DORA compliance

Enhanced visibility and control: AlgoSec provides visibility into applications and security policies across hybrid and multi-cloud environments. This helps financial institutions reduce risks, address vulnerabilities, and meet DORA's resilience requirements.

salesforce

G



Automated compliance and audits: Manual firewall rule recertification is time consuming. AlgoSec automates the process, saving up to 30% on compliance time while ensuring continuous compliance through applicationbased recertification. This approach also ensures continuous compliance, even as applications evolve.

							(Palaborner	
Applications 4	Exchange		NAME RESULTS VALUE	Analisty Atlant Atlanty (DS				Constant in Dig serve
E Solway		lares	Destration	lates				
APLOBATE The Party			(*) *)	a dala Mar				
E SuprON. E Presser Management	4 flows found						Store canto	aben abquetures
Payl-Darley Insettory that agreese	🖌 Appleation thesis (2)							The Property Assess
E insidefing	1 Band	1 Searce	(Berl	- Destination	Not work Applic	ather Service	Campion's	
Robert Balancesi B. Carl		El velloche	2.89	E LACER SAME AND A LAND	a M2	2 M/G		0
Englister Partie	4	an Care, Inc., Mo an Care, No., Mo	1.879) (B. internet	() A Ay) <i>p</i> 1011	Ciert Asses to F	- 0
	2	B. (1), (1), (1), (1), (1), (1), (1), (1),	(i) x ==	1 100,00,00 100,00,00	1 8 .49) ja aitas	Provide to West	
	5 Marid Flows (0) + 0	and street from						
	v Subscribed Howe (1)	· Add and an iterations						E forde ford
	1 Marci	1 Seuro	1 1041	- Defination	The section of the se	attan T Service	Lanners	
-	е — то и	10 (10, 10 million)	B) 3.54	🖉 bisenal 201 Servers	: Birt	. @ 011	Publick Del Laris other application	

Audit-ready reports: AlgoSec generates automated, audit-ready reports that provide real-time visibility into network security policy changes and potential risks. These reports help organizations continuously monitor their compliance status, making it easier to provide timely documentation to regulatory bodies and pass audits with ease.

				DORA Complia	ance Report				
Criterion		lating	Details						
Risk Profile		AlgoSec Standard							
RFC 1913 IP addresse	a l	Trusted							
Trusted Traffic		08	0 Trusted Traffic Rule						
Diffline Security Scan P	leselts								
The AlgoSec Firewall Ar	adyter provides an Offline Security Scan o	f the organization's devices. with the Common Wilmerability Scoring Syste	an POSS of Maser						
	7.0-10.0								
	4663						*	C) C Rolounch to	
	10.00				https://10.20.230.11/algosec-ui/report/afa-3608/regulatory-compliance		¥	C) 🥑 Resource to	
	2.0-3.9 The	following table lists all the risk items that wer each risk item. The Status column indicates or	re searched for according to the Risk Assessment Orderia	Cip Capgemini 88					
	1.1	he risk item was not found		******	and the second				
		he risk item was found se risk item was found, but it is a special case	of a more general risk item. Only the more general risk it		one-armed-vr Regulatory Compliance				
Carlo	Muk Seculation	_		4					
1 01	"Imp" Services can unlike your red	0404			DORA Compliance Report	70% Compliant		Export/Print PDF	
2. 102	TCP on all ports can enter your	oetwork		6 HOME	and the second				
3 103	UDP on all ports can enter your	network		U Auses	The AlgoSec Firewail Analyzer DORA Compliance report is based on the Digital Operational Resilience Act (DORA), Regulation (TU) 2022/2554, alms to strenction subersecurity across the EU Rhandal sector.				
4 107	Risky Microsoft services can ent	or stan per a central por manera			As of March 13' 2024, a new Delegated Regulation supplements DORA by establishing technical stand ands for ICT risk management, detailing tools, motions, and positions required for compliance. TBA (impress Compliance exercised)				
5 001	The Company between Street								
6 84	Telest can enter your network				 Title is General Principle Title 1: Further Hammerication OFICT Risk Management Tools, Netbods, Processor 	And Deliving In Accordance With Leticle 15.			
7. 109	Own 256.IP addresses can be re	actual by SMTP		CHANCES	Of Regulation (Eu) 2022/2554				
8. 110	Over 2561P addresses can be re	ached by DNS/UDP			 Title HL Simplified ICT Risk Management Fremework For Financial Entities Referre 2022/2554 	o to in whole 16(1) or segments (01)			
0. 114	TCP on over 2000 ports can ente	ir your network			General				
	Over 2561P addresses can be re	ached by DNS/TCP							
10. 116				D VPN	Device: VR-Adele.1-1_vsys1_one-armed-ur (40.40.1.6) Versioe: perceama 10.0.0				
10. 116 11. 117	MSSQL can enter your network								
	MSSQL can enter your network Database access services can er				Policy: 10_156_0_157_Adele_1_1_vsys1_one_armed_vr.panorama				
11. 117				= POLICY	Policy, 10, 154, 0, 151, Adee, 1, 1, Vsyst, one, Ameri, V. Janorana Date: 2024-12-30				
11. 117 12. 120	Database access services can er								

Accelerated incident response: AlgoSec's automation capabilities allow for quick response to security incidents by identifying and isolating affected applications. This helps financial institutions meet DORA's fast recovery requirements, minimizing disruptions to business operations.

CRM (Pend		VAL NERMANTY	ISSS ACONTRISS					
A								
27								
		-				_		10/06/2228
SCHREEP SCHEEP DE					2 1		1	
Instained Strutes of	> C Time Dock Server	80 -				2		10/95/2019
								Internet.
	7 A TATEPOLISTICS	97						
	CRM (Pend December) 8/205	COMM (Pending Implementation)	CRM (Perdig Inplanentation) common and source of the source of	C CRM (Predig Implementation)	CRM Procing implementation) Common and	C CRM (Precing Implementation) Denote and total control of the second	C CRM (Procing traphenetration) December 2000 Sector 2000 D C CRM (Procing traphenetration) D C CRM (Procing traphenetration) D C CRM (Procing traphenetration) D D C CRM (Procing traphenetration)	C CRM (Perding Implementation) Demonstration (Complementation) Demonstration (Complementation)

Application-centric compliance: Rather than focusing solely on network infrastructure, AlgoSec takes an application-first approach, ensuring that business-critical applications are both protected and compliant. This alignment with real-time application demands supports DORA's emphasis on operational resilience and data protection.

As DORA compliance begins to be enforced, financial institutions need to evaluate and optimize their network security and compliance strategies. AlgoSec offers the tools needed to achieve resilience, protect sensitive data, and simplify the compliance process through automation. With AlgoSec, organizations can ensure business continuity, reduce operational risks, and be audit-ready at all times.

With AlgoSec, financial institutions can confidently navigate the complexities of DORA and position themselves for long-term operational resilience and regulatory compliance.

About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to secure application connectivity by automating connectivity flows and security policy, anywhere.

The AlgoSec platform enables the world's most complex organizations to gain visibility, reduce risk, achieve compliance at the application-level and process changes at zero-touch across the hybrid network.

Over 1,800 of the world's leading organizations trust AlgoSec to help secure their most critical workloads across public cloud, private cloud, containers, and on-premises networks.



 \bigcirc AlgoSec Inc. All rights reserved. AlgoSec and the AlgoSec logo are registered trademarks of AlgoSec Inc. All other trademarks used herein are the property of their respective owners.



<u>AlgoSec.com</u>