Distology. | okta

3

Ways Identity helps with Compliance for DORA & NIS 2

Find out more

Distology. | okta

#1 PROTECT NETWORKS AND SYSTEMS FROM CYBER THREATS

NIS 2 requires digital service providers to **implement strict security measures** to prevent cyber threats and report significant cyber incidents. By ensuring only authorised individuals or systems can access a network or system, **Identity significantly reduces the risk of a cyberattack.**

Distology. | okta

#2 STRENGTHEN OPERATIONAL RESILIENCE

DORA aims to **enhance the operational resilience** of digital service providers by enforcing a risk-based approach. Digital Identity management **reduces the risk of unauthorised access** by ensuring only authorised individuals can perform critical functions.

Distology. | okta

#3 MORE ROBUST DATA ACCESS PROCESSES

Effective digital identity management is crucial for data protection, incident reporting, and compliance with **DORA** and **NIS 2**. Access management enables organisations to **track access, provide auditable evidence, and automate processes efficiently.** This is vital for compliance with **DORA** and **NIS 2**.

Distology. | okta

Want To Find Out More?

Talk to one of our cybersecurity experts to find out how Distology can help your customers with **regulations and frameworks**.

✉ INFO@DISTOLOGY.COM