HOXHUNT

NIS 2 Checklist

This checklist helps the CxO and Board of Directors get on the same page with the CISO to optimize NIS 2 compliance.

Topics for CxO level to check

	Have we nominated a Cybersecurity accountable (CISO) who has the proper resources to fulfil the NIS 2 requirements?
	Have we clearly communicated with the CISO and agreed on why Cyber Security is important for our company?
	Have we reviewed the CISO's plan and Cybersecurity risk management measures, and agreed upon KPIs to measure its execution and resourcing?
	Have all of our CxO's participated in NIS2-related Cybersecurity training to understand our role with this regulation?

Topics for the CISO to include in their plan

	Do we have an effective incident notification process that enables us to give early warning within 24h to authorities and follow the tight schedule defined by the directive?
	Do we have an effective cybersecurity risk analysis process that directs the investments and ensures continuous development?
	Do we have effective business continuity measures in place to support our critical services?
	Do we have a list of critical suppliers to our company, and have we agreed with them on how they will enable our business continuity?
	Do we have a reliable process to secure all new assets and maintain their security? (Vulnerability and hardening management)?
	Do we have policies and procedures to assess the effectiveness of cyber security risk management measures?
	Do we have effective cybersecurity training for our employees that is relevant and delivers measurable results?
	Are we clear on using cryptography with our solutions?
	Do we have clear access control policies, and do we have a clear asset registry?
	Do we use multi-factor or continuous authentication where appropriate and are our communications channels & solutions properly secured?