FUCHS GRUPPE

RECOMMENDATION / REFERENCE LETTER

Project: Cybersecurity Consulting for the Implementation of NIS2 Requirements

We, FUCHS CONDIMENTE RO SRL, a Romanian legal entity, with registered office at 41–43 Strada Nordului, Curtea de Argeș 115300, registered with the Trade Register under no. J2001000189038, having VAT number RO 13807887, hereby confirm our collaboration with S.C. SECTIO AUREA S.R.L., with registered office in Romania, Bucharest, 23C Calea Vitan Street, Vitan Business Center, Room 2, Sector 3, postal code 031281, identified by VAT number RO18334569, Trade Register no. J40/1426/2006, under Contract no. 1146 dated 14.02.2025, performed during the period 14.02.2025 – 13.08.2025 (6 months).

Within this project, S.C. SECTIO AUREA S.R.L., through the involved expert Eduard Mădălin Bratu, provided specialized consulting services for aligning our organization with the requirements of the NIS2 Directive, covering a comprehensive journey from governance and compliance to operational resilience. The project commenced with the establishment of information security governance, including the clarification of the role and responsibilities of the NIS2 Officer/Information Security Officer, the adjustment of reporting lines towards management, and the operationalization of the accreditation process, including supporting documentation, the accreditation file, and the related accreditation decision. In parallel, measurement and reporting mechanisms were defined through the establishment of key security indicators and an evaluation methodology, ensuring that management reporting is relevant, measurable, and easy to interpret, including periodic presentation sessions and trend analysis.

To ensure sustainability of compliance, the consulting team defined and documented the NIS2 compliance assessment process and the audit/self-assessment framework, providing initial training and support for drafting the first assessment deliverables, depending on the compliance model selected by the organization. An important pillar of the project was the strengthening of the security culture, achieved through the definition of the security education and awareness program and the integration of security requirements into employee relations, including updates to relevant internal documentation and the implementation of training mechanisms, knowledge verification, and skills transfer to the internal responsible function, including a train-the-trainer approach.

In addition, the project included the execution of a Business Impact Analysis (BIA) to identify critical processes, dependencies, and recovery priorities, with the establishment of RTO/RPO targets and recommendations for integrating the results into business continuity and disaster recovery planning. Based on the inventory and analysis of the information system architecture, information flows, and vulnerability assessments, a comprehensive risk analysis was performed, and the risk register was developed, including threat scenarios and probability/impact assessments, as well as recommendations for technical and organizational measures, substantiated by feasibility considerations and functional requirements where applicable. The vendor risk assessment component complemented this phase through the analysis of third-party supplier contracts, security obligations, SLAs, and audit mechanisms, resulting in a clear view of ecosystem-related risks and corresponding mitigation actions.

FUCHS GRUPPE

At the same time, information classification requirements were addressed through information inventory, definition of confidentiality levels, guidance on labeling and protection measures, including a GDPR compliance analysis on relevant components. In the area of access control, identity and access management processes were defined and enhanced, including remote access and privileged accounts, with approval workflows, periodic reviews, and verification mechanisms, as well as recommendations for digitalization through specific solutions (IGA/PAM/SSO), where appropriate. Furthermore, the project aimed to strengthen systems management through recommendations on network segregation, review of traffic filtering configurations, cryptographic protection, and security baselines, including exception management and alignment guidance with recognized standards for critical infrastructures.

From an operational perspective, processes for detection and incident response were defined, covering monitoring, triage, escalation, isolation, evidence collection, remediation, recovery, and follow-up, together with directions regarding SOC capability organization and integration into relevant reporting workflows. Finally, the results of the BIA and risk analysis were used to shape the continuity framework, including guidance for defining and operationalizing a Disaster Recovery Plan (DRP), with roles, responsibilities, scenarios, and testing and update mechanisms.

Throughout the collaboration, S.C. SECTIO AUREA S.R.L., as well as the expert Eduard Mădălin Bratu, demonstrated solid expertise, a structured approach, and a strong orientation towards auditable and operationally applicable deliverables, contributing to the increase of governance, control, and resilience maturity in the context of NIS2 requirements. Based on the above, we recommend S.C. SECTIO AUREA S.R.L. and Eduard Mădălin Bratu as a consulting partner for projects aimed at implementing NIS2 requirements and strengthening cybersecurity and operational continuity.

Yours sincerely,

FUCHS CONDIMENTE RO SRL
Cătălin Arsene / IT Manager

09.02.2026