NIS-2 Compliance Checklist

1. Entity Classification under NIS-2

- **NIS-2 Category: Important Entity** – Kautschuk Group falls under NIS-2's *important entities* category (not "essential"). It operates in **research** and **industrial manufacturing** sectors, which NIS-2 lists as important entities for medium/large enterprises. The directive's size threshold for medium/large enterprises is ≥50 staff or >€10 million turnover. (NIS2 Directive and the SME Recommendation). *As an important entity, Kautschuk Group must implement all NIS-2 security measures and reporting duties, though supervisory oversight and maximum fines are somewhat lower than for essential entities* (Who does NIS2 apply to).

2. Cybersecurity Governance & Accountability

- **Executive Accountability:** Ensure top management (board or directors) **formally approves the cybersecurity risk management program** and oversees its implementation (NIS 2 Directive, Article 20: Governance). Document this in board meeting minutes or policies. Management is accountable for NIS-2 compliance (NIS 2 Directive, Article 20: Governance), so establish clear reporting to the board on security status.

- **Assign Security Leadership:** Appoint a qualified **Chief Information Security Officer (CISO)** or security coordinator responsible for NIS-2 compliance. This role should coordinate risk assessments, implement controls, and act as the point of contact with regulators. Define their authority and resources in a charter approved by management.

- **Management & Staff Training:** Provide **cybersecurity training for management** and key decision-makers (NIS 2 Directive, Article 20: Governance) so they can identify risks and understand security practices. NIS-2 explicitly requires management bodies to undergo training (NIS 2 Directive, Article 20: Governance). Also offer regular security awareness training to all employees (phishing prevention, safe data handling, OT safety procedures) to instill basic cyber hygiene and policy compliance across Kautschuk Group.

- **Security Policy and Procedures:** Establish an **Information Security Policy** (approved by management) that defines Kautschuk Group's security objectives, roles, and rules. Include sub-policies for areas like acceptable use, remote access, OT network usage, and incident response. Ensure policies cover both IT and OT environments and are aligned with NIS-2 requirements (NIS 2 Directive, Article 21: Cybersecurity risk-management measures). Review and update these policies at least annually or upon significant changes.

3. Cybersecurity Risk Management Program

- **Implement an ISMS:** Develop an **Information Security Management System (ISMS)** aligned with international standards (e.g. ISO/IEC 27001) to manage cybersecurity risks. This system formalizes risk management processes: asset inventory, risk assessment, control implementation, monitoring, and continuous improvement. Following ISO 27001 or equivalent will help ensure all NIS-2 control areas are addressed (NIS2 Directive: German government adopts draft NIS2 Implementation Act).

- **Risk Assessment:** Conduct a comprehensive **risk analysis** covering all critical assets and processes (NIS 2 Directive, Article 21: Cybersecurity risk-management measures). Identify assets (including research data, IT systems, and OT/industrial control systems), threat scenarios (e.g. malware, insider abuse, supply chain attacks), vulnerabilities, and potential impact (e.g. data breaches, production downtime). Evaluate risks and document them in a risk register. *Include both IT and OT domains in this assessment*, noting that OT systems may have unique risks (e.g. safety impacts from disruptions).

- **Risk Treatment & Mitigation:** For each identified risk, decide on treatment (mitigate, transfer, accept, or avoid). Implement **risk mitigations** proportional to the risk level (NIS 2 Directive, Article 21: Cybersecurity risk-management measures) – e.g. apply security patches, add network segmentation, improve access controls (detailed below). Prioritize high-impact risks affecting confidential data and production operations. Track risk treatment actions and have management sign off on acceptable residual risks.

- **Supply Chain Risk Integration:** Incorporate **supply chain risks** into the risk management process (NIS2 Directive: German government adopts draft NIS2 Implementation Act). Identify critical suppliers (IT service providers, cloud hosts, industrial equipment vendors, etc.) and assess how their cybersecurity posture could affect Kautschuk Group (NIS 2 Directive, Article 21: Cybersecurity risk-management measures). For example, evaluate the risk of a supplier software compromise impacting your operations. Update the risk register with supplier-related risks and ensure mitigation measures (see Supply Chain Security section) are in place.

- **Documentation & Review:** Maintain documentation of all risk assessments, decisions, and implemented controls (NIS2 Directive: German government adopts draft NIS2 Implementation Act). NIS-2 compliance demands evidence of a risk-based approach. Review and update the risk assessment at least annually or whenever major changes occur (new OT system, new branch office, emerging threat in the industry). Regularly report risk status to management and refine the program as needed.

4. Technical and Operational Security Measures

- **Asset Management & Network Segmentation:** Create and maintain an **inventory of assets** – list all hardware, software, data repositories, and network components, including OT equipment. Classify assets by criticality and sensitivity (e.g. confidential R&D data, production line controllers). Use this inventory to enforce protections. **Segment networks** to protect critical systems: for example, separate the OT network from the corporate IT network via firewalls/DMZs, and restrict communication to only necessary flows. This limits the impact of malware spreading from office IT to industrial control systems. Regularly update network diagrams and asset lists as the environment changes.

- **Access Control & Identity Management:** Implement strict **access control policies** for both IT and OT systems (NIS 2 Directive, Article 21: Cybersecurity risk-management measures). Apply the principle of least privilege – each user/account gets only the minimum access needed. Use unique accounts (no shared logins) and strong authentication for all employees and third-parties.

- **Enforce Multi-Factor Authentication (MFA)** for remote access, privileged accounts, and important applications (NIS 2 Directive, Article 21: Cybersecurity risk-management measures) (e.g. require one-time tokens or certificates in addition to passwords). Regularly review user access rights (at least quarterly) and promptly revoke access for departing staff or role changes. For OT systems, tightly control access to control interfaces and engineering workstations, possibly using jump hosts with MFA for any OT network access.

- **Cryptography & Data Protection:** Establish **policies on cryptography and encryption** usage. Ensure sensitive data (e.g. research results, personal data, proprietary production data) is encrypted at rest (using disk/database encryption) and in transit (TLS for network communications) (NIS 2 Directive, Article 21: Cybersecurity risk-management measures). Use industry-standard algorithms and secure key management (e.g. centralized key vaults, regular key rotation for critical keys). If applicable, utilize secure voice, email, and messaging solutions for confidential communications (NIS-2 encourages secured communication systems for voice/video/text). Document approved cryptographic protocols in the security policy and disable outdated ones.

- **Secure System Configuration:** Apply **secure configuration baselines** to all systems. This includes hardening servers and PCs (disable unused services, enforce strong password policies, apply least privilege file permissions), securing network devices (change default credentials, use secure management interfaces), and locking down OT controllers (apply vendor security guidelines, disable unused physical ports). Use configuration management tools or group policies to enforce baseline settings across IT assets. For OT equipment, work with engineers to apply security configurations that do not impede safety.

- **Protective Technology Deployment:** Deploy key **security technologies** to protect the network and endpoints. At minimum, use up-to-date anti-malware/EDR on all endpoints and servers, perimeter firewalls to filter traffic, and Intrusion Detection/Prevention Systems (IDS/IPS) to monitor network traffic for attacks. For OT networks, consider industrial IDS that can detect anomalous control commands. Implement network access control (NAC) to prevent unauthorized devices from connecting. Ensure critical systems have physical security controls as well (restricted access to server rooms and control panels).

- **Vulnerability Management & Patching:** Establish a **vulnerability handling process** for IT and OT systems. Continuously monitor for newly disclosed vulnerabilities (subscribe to vendor alerts, CERT advisories). **Promptly apply security patches** and updates to software, operating systems, and firmware – with priority on high-risk vulnerabilities. For OT systems where patching can be slower due to operational constraints, develop a schedule and compensating controls (e.g. increased monitoring or network isolation until patches can be applied). Use automated vulnerability scanning tools on IT systems and periodic manual assessments on OT equipment to identify unpatched flaws. Keep a log of vulnerabilities found and mitigation actions taken. Additionally, establish a **coordinated vulnerability disclosure** procedure – e.g. publish a contact email or form on your website so external researchers can report security issues, and have an internal team ready to respond and fix reported bugs.

- **Basic Cyber Hygiene Practices:** Enforce **baseline cybersecurity best practices** for all staff and systems. This includes using strong passwords or passphrases (and a password manager where possible), regular password changes or passwordless auth with MFA, locking computers when unattended, and keeping work devices updated. Ensure endpoint devices have disk encryption enabled and automatic screen lock. Limit use of personal devices or implement Mobile Device Management (MDM) with security controls for any BYOD. Regularly remind employees of safe practices (through awareness campaigns). Perform routine **backup management** for critical data (as part of continuity): verify backups complete successfully and are protected from tampering (e.g. offline or immutable backups). Test restore procedures to verify integrity of backups.

- **Operational Technology (OT) Security:** Apply tailored security controls to **industrial control systems** and OT environments. Ensure a clear inventory of OT assets (PLCs, SCADA, HMIs, etc.) and identify critical production processes. **Isolate OT networks** from general IT (no direct internet access from OT; use jump servers or VPN with MFA for engineers connecting to OT). Work with control system vendors to keep firmware up to date and apply security patches during maintenance windows. Implement monitoring for OT (detect unusual traffic or device behaviors that could indicate cyber intrusion or malfunction). Have strict procedures for any remote access to OT (e.g. vendor maintenance connections) – use secure methods and supervise sessions. Train OT personnel on cybersecurity incidents (e.g. how to recognize signs of cyberattack on HMI screens or control anomalies). In risk assessments, consider worst-case OT attack scenarios (like a ransomware causing plant shutdown) and put in place preventive and contingency measures accordingly.

- **Effectiveness Testing:** Define **procedures to assess the effectiveness** of security controls on a regular basis. This can include periodic security audits, technical security tests such as penetration testing of corporate networks, and conducting scenario-based drills (for both IT and OT incidents). Use the results to adjust and improve controls. For example, run phishing email tests to gauge employee vigilance, or have an external consultant assess the network segmentation. NIS-2 requires entities to have policies for evaluating how well their cybersecurity measures perform, so develop metrics (e.g. % of systems patched within SLA, number of incidents detected internally vs by third-parties) and report these to management for review.

5. Incident Detection and Response

- **Continuous Monitoring:** Implement **security monitoring and detection capabilities** to rapidly identify incidents. Deploy a Security Information and Event Management (SIEM) system or similar log management solution to aggregate and analyze logs from servers, network devices, security tools, and OT systems. Configure alerting for suspicious activities (e.g. multiple failed logins, unusual after-hours OT commands, large data transfers). Consider an Intrusion Detection System (IDS) or Managed Detection & Response (MDR) service to watch for advanced threats. Ensure that **both IT and OT environments are monitored** – for OT, tailor detection rules to the industrial protocols in use. Regularly review alerts and tune the monitoring systems to reduce false positives. The goal is to detect anomalies early so that response can begin and NIS-2 reporting deadlines can be met.

- **Incident Response Plan:** Develop and maintain a **documented Incident Response Plan (IRP)** that outlines the steps to take when a security incident is suspected or confirmed. Include clear roles and responsibilities (e.g. who is the incident manager, who contacts BSI/authorities, who handles technical containment, who communicates to customers, etc.). The plan should cover detection, analysis, containment, eradication, recovery, and post-incident review. Include specific procedures for likely scenarios such as malware infection, ransomware on an OT system, data breach of research info, or DDoS on online services. *Ensure the plan meets NIS-2's reporting requirements (detailed next)*. Test the incident response plan at least annually with simulated drills (e.g. a tabletop exercise of a cyber incident affecting production) and refine it based on lessons learned.

- **NIS-2 Incident Notification: Establish a procedure to report incidents to authorities in the mandated timeframes.** Under NIS-2, any *significant incident* (one causing substantial service disruption or impact) must be reported to the national CSIRT or competent authority (BSI in Germany) in stages (NIS 2 Directive, Article 23: Reporting obligations):

    - **Early Warning (within 24 hours):** Within 24 hours of becoming aware of a significant incident, send an initial notification. Include whatever is known at that time – e.g. that an incident is happening, suspected cause (if known whether it's malicious), and if it might have cross-border impact. Prepare a template for this "early warning" report to ensure speed.

    - **Incident Notification (within 72 hours):** Within 72 hours of awareness, submit a more detailed incident report. This should update information from the early warning and provide an initial assessment of severity and impact. Include technical details such as the affected systems, the type of attack or root cause if identified, and any indicators of compromise (IOC) known. Have an incident report form ready to be filled during an incident (covering NIS-2 required fields).

    - **Intermediate Updates:** Be prepared to provide **interim status reports** if the CSIRT/BSI requests them. For major incidents, the authority may ask for ongoing updates as you work on containment and recovery. Assign someone on the incident team to interface with the BSI regularly.

    - **Final Report (within 1 month):** No later than one month after the 72h notification, submit a **final incident report**. This must include a detailed post-incident analysis: the full scope and impact of the incident, root cause (what vulnerability or failure led to it), what threat actor or mechanism was involved, and what mitigation measures have been applied or will be implemented to prevent recurrence. Essentially, do a thorough **post-mortem** and document it for the regulator. If the incident is still ongoing at the one-month mark, provide a progress report and agree on a timeline for the final report.

    - **Record-Keeping:** Keep an internal log of all incidents (even minor ones). For each, document dates/times of detection, actions taken, communications, and lessons learned. This will not only aid in creating the reports above but also demonstrate a history of compliance and improvement if audited.

- **Notify Affected Parties:** If an incident or emerging cyber threat could significantly affect customers, partners, or service recipients, **inform them without undue delay**. NIS-2 requires entities to notify service recipients of significant incidents that may adversely affect the services , as well as to communicate measures those users should take in response to significant cyber threats. Prepare templated communications for incident notifications to clients (e.g. "Our services are experiencing an outage due to a cybersecurity event, here's what you need to know..."). Coordinate these communications with legal/PR teams to ensure transparency while managing liability and trust. Also, ensure your incident plan includes when and how to publicize incidents if instructed by authorities (the BSI can instruct you to inform the public in certain cases).

- **Leverage CSIRT Guidance:** Contact and seek guidance from your sector's Cyber Security Incident Response Team (CSIRT) if needed. In Germany, BSI or sector-specific CSIRTs can assist during major incidents. Share indicators of compromise with them to help broader defense. Participate in any threat intelligence sharing communities relevant to your industry – while voluntary, this can improve detection and response (aligns with NIS-2's encouragement of information sharing).

6. Supply Chain Security Management

- **Inventory of Suppliers:** Create a register of all key **suppliers and service providers** that support your IT or OT operations. This likely includes cloud hosting providers, software vendors (ERP systems, research data software), equipment manufacturers for production systems, managed service providers, etc. For each supplier, identify what product/service they provide and how a compromise at that supplier could impact your organization (e.g. if your cloud provider is down or hacked, what is the effect? If a vendor's software update is malicious, what could it breach?). This inventory will feed into supplier risk assessments.

- **Supplier Risk Assessment:** Perform **cybersecurity risk assessments for critical suppliers** . Evaluate their security posture: Do they have certifications (ISO 27001, TISAX for automotive, etc.)? What is their history of breaches? What security measures do they advertise? You may send them security questionnaires or rely on industry ratings. Pay extra attention to suppliers with direct connections to your network or sensitive data access (e.g. an outsourced IT admin firm or an OT maintenance contractor). NIS-2 mandates considering vulnerabilities of each direct supplier and the overall quality of their security practices. If a particular vendor is high risk, develop contingency plans (e.g. be ready to switch to an alternative, or ensure additional monitoring of that vendor's accesses).

- **Security Requirements in Contracts:** Update procurement and vendor contracts to include **cybersecurity clauses**. Require that suppliers adhere to "state of the art" security measures and notify you promptly in the event of any incident that could impact your organization. For example, vendors should agree to patch known vulnerabilities in their products within a defined timeframe, and service providers should maintain access controls and not subcontract without consent. Include right-to-audit clauses or request security assessment reports from key suppliers periodically. Ensure NDAs and data processing agreements (if personal data is involved) are in place to cover confidentiality of shared information.

- **Supply Chain Attack Prevention:** Verify the integrity of **software and updates** from suppliers. Use digital signatures to validate software patches/firmware coming from vendors before applying them to OT systems. Maintain a checksum/verification process for any third-party libraries or open-source software in use. For hardware, procure from trusted sources and follow any BSI guidance on approved suppliers for critical components. (*Germany-specific:* follow the IT-SiG rules on critical components – e.g. if you use certain critical telecom or OT components, ensure they are approved or notify BSI as required by German law.) Limit third-party remote access: if vendors need to access your systems for support, enforce secure methods (VPN with MFA, time-limited accounts) and supervise their activity.

- **Monitoring Supplier Performance:** Continuously **monitor supply chain conditions**. Stay alert to news of breaches or vulnerabilities involving your vendors. For instance, if a major supplier (cloud or software) suffers a cyber incident, quickly assess impact on your systems and data; communicate with that supplier to get details and mitigations. Keep an eye on threat intelligence regarding supply chain attacks (ENISA and other bodies often issue warnings about specific threat trends). NIS-2 also calls for considering results of any *Union-wide coordinated risk assessments* for critical supply chains – for example, if the EU flags certain technology (like 5G infrastructure or cloud services) as high-risk, factor that into your strategy (possibly by diversifying suppliers or imposing stricter controls on those products).

- **Alternative & Contingency Plans:** For critical services or products, have **backup suppliers or internal solutions** ready in case a primary supplier is compromised. For example, if you rely on one cloud provider, consider a strategy to migrate to another or operate on-premises temporarily if needed. If a particular chemical or component for production is sourced from one vendor, identify alternate sources. This business continuity aspect of supply chain security will reduce dependence on any single point of failure. Include such scenarios in your business continuity plan (Section 7) to ensure you can continue operations if a supply chain disruption occurs due to cyber issues.

7. Business Continuity & Disaster Recovery

- **Business Continuity Planning:** Develop a **Business Continuity Plan (BCP)** that addresses how Kautschuk Group will maintain or restore operations during and after a cybersecurity incident. Identify critical business processes (e.g. production line operation, research data analysis, customer order fulfillment) and outline how to keep them running in degraded modes if IT/OT systems are hit by an incident. For example, plan for possible manual workarounds or temporary process halts in production with safety as priority, or shifting workloads to an unaffected location. The BCP should map to various incident scenarios (ransomware, extended IT outage, etc.) and assign responsibilities for decision-making during a crisis. Make sure the plan considers loss of ICT services (what if certain servers or networks are unavailable) and includes communication plans to staff and customers.

- **Disaster Recovery (DR):** Establish a **Disaster Recovery plan** focused on restoring IT systems and data after disruption. Define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for key systems – e.g. “ERP system must be restored within 24 hours with less than 1 hour of data loss.” Set up backup **sites or cloud DR environments** if feasible for critical servers. Implement regular data backups (daily or more frequent for critical databases) and **backup management processes**: verify backups, encrypt backups, and store backups offline or in a separate network segment to protect them from ransomware. Document detailed restoration procedures for systems (who will do what to rebuild servers or deploy VMs from backups). Test the DR procedures at least annually to ensure your team can meet the RTOs (for instance, do a simulation where you restore a backup of an important server and measure the time).

- **Crisis Management & Communication:** Create a **Crisis Management plan** as part of business continuity that deals with high-level coordination and communication during a major incident. This plan should establish a Crisis Management Team (including executives, communications/PR, legal, IT/OT leads) who will convene for serious incidents (e.g. a breach that stops production or leaks sensitive data). Define an internal escalation protocol: how and when an incident is escalated to this team. Prepare communication templates for internal updates (keeping employees informed of what to do) and external statements (for media or customers, aligned with any regulatory disclosure requirements). Identify points of contact for external stakeholders (e.g. major clients, law enforcement, regulators) and decide how communications will be handled if normal channels (email, corporate phones) are down – e.g. maintain an out-of-band contact method like phone trees or personal emails. Practice this by conducting periodic crisis exercises.

- **OT Systems Continuity:** Specifically address **business continuity for OT systems** and production lines. Determine how you will maintain safety and core operations if control systems fail or are compromised. For example, develop standard operating procedures to safely shut down equipment if monitoring systems go dark, or to run the plant in a manual mode if possible. Ensure backup of critical control configurations (so they can be reloaded on new hardware if controllers are lost). Store copies of PLC programs and SCADA configurations offline and securely. Include OT engineers in continuity planning – they should know how to recover control systems from scratch if needed. If your production is distributed across multiple sites, plan for shifting production to unaffected sites when feasible.

- **Regular Testing and Updating: Test the BCP and DR plans** regularly. Conduct drills such as simulated ransomware attacks that invoke both IT recovery and crisis communication, or a simulation of an OT outage. After each test or real incident, update the plans to fix any gaps discovered. Also review the BCP/DR plans at least yearly to account for organizational changes (new systems, new locations, changes in personnel). Ensure copies of the plans are accessible even during an incident (e.g. stored in hard copy or on an off-network device) in case normal IT access is disrupted.

8. Regulatory Compliance and Cooperation

- **Registration with Authorities:** Fulfill Germany-specific registration duties. **Register Kautschuk Group with the German Federal Office for Information Security (BSI)** as an entity under NIS-2, if required by the German transposition law. (The draft German NIS2 Implementation Act requires in-scope entities to register with BSI within 3 months of coming into scope.) Provide details such as the company's sector, contact persons, and any other required information. Keep this registration updated if your company details change. This ensures the authorities know you are under NIS-2 regulation and can send you relevant information or guidance.

- **Liaison and Point of Contact:** Designate a **NIS-2 single point of contact** for regulators. In practice, this could be the CISO or Compliance Officer who will interface with the BSI. Ensure this person's contact info (phone, email) is shared with BSI through the registration. They should be prepared to receive alerts or requests from BSI/CSIRT and coordinate Kautschuk Group's response. Also, monitor communications from BSI (or sector CERTs) for any threat notifications or guidance they send out.

- **Incident Reporting Compliance:** As detailed in section 5, make sure your incident response procedure aligns with the **official reporting channels and formats** in Germany. Know **how to submit incident notifications** to the BSI or CERT-Bund (e.g. via the BSI's incident reporting portal or email, as directed by BSI guidelines). Test the reporting process (even if just a drill) so that during a real incident the team can file reports without delay. Keep copies of all reports sent to regulators as part of compliance records.

- **Cooperate with Regulatory Oversight:** Understand that as an important entity, the company is subject to **ex-post supervisory enforcement**. This means the BSI might investigate compliance after incidents or if they suspect non-compliance, rather than continuously monitoring you. Nevertheless, be fully cooperative if the BSI contacts you. Respond to information requests (they may ask for details on your security measures or an explanation of an incident). If the BSI issues any **instructions or orders** (e.g. to fix a specific deficiency), address them promptly. Document all such interactions.

- **Audit and Evidence Preparation:** Be prepared for the possibility of **audits or spot-checks** by BSI. While routine audits are more likely for "essential" (very important) entities, BSI can require important entities to undergo a security audit in certain cases.

Maintain an audit-ready posture:

  - Keep an organized repository of all security policies, risk assessment reports, training records, incident logs, and technical security control documents. This will make it easier to demonstrate compliance.
  - If feasible, **obtain an independent audit or certification** of your cybersecurity (for example, ISO 27001 certification) to have third-party attestation of your controls. This can satisfy some audit requirements and shows good faith in compliance.
  - Conduct **internal audits** or self-assessments against the NIS-2 requirements checklist (this document can serve as a basis) at least annually. Identify any gaps and remediate them proactively. Retain the results as evidence of continuous improvement.

- **Enforcement Preparedness:** Be aware of the penalties and ensure management is committed to avoidance of those. Under NIS-2 (as implemented in Germany), important entities face fines up to €7 million or 1.4% of global turnover for serious infringements. Essential (very important) entities would face up to €10 million or 2%, but as an important entity you still have significant fines at stake. Additionally, Germany's law increases **personal liability for executives** on cybersecurity failures. Communicate this to senior leadership to reinforce the importance of compliance. Have legal counsel ready to advise in case of any enforcement action. Ensuring all the above measures are in place and well-documented is the best way to **demonstrate due diligence** and avoid or mitigate penalties if the BSI examines your case.

- **Ongoing Compliance Monitoring:** Treat NIS-2 compliance as an ongoing process. Keep track of updates in German regulations or guidance (BSI might release sector-specific rules or updates to the law). Assign responsibility (perhaps the compliance officer) to monitor any changes in NIS-2 interpretation or new security standards (e.g. new **European cybersecurity certification schemes** relevant to your industry, as NIS-2 encourages their use (NIS 2 Directive | Articles)). Update your compliance program accordingly. Regularly report the state of compliance to the board (e.g. annual NIS-2 compliance report outlining risk posture, controls, incidents, training completed, etc.) to keep accountability at the highest level.

By following this comprehensive checklist, Kautschuk Group addresses all relevant **NIS-2 obligations** – from governance and risk management through technical controls, incident handling, supply chain security, continuity planning, and regulatory compliance. This will significantly enhance Kautschuk Group's cybersecurity resilience and ensure adherence to both EU NIS-2 requirements and Germany's specific implementation rules.