Key Responsibilities

- Leading internal and external security audits in the area of information security (ISO2700x,)
- Driving ISO program implementation and its stakeholders
- Leading information security risk management incl. the identification, assessment, monitoring and mitigation of security risks
- Creating and managing security standards, incl. related processes as well as their maintenance and continuous improvements
- Assessing current solutions, suggesting then tracking identified upgrades and improvements to information security
- Provide continuous assessments of our business continuity preparedness
- Serve as a point of contact for the organization regarding information security processes and policies
- Subject matter expert on the group security incident response handling
- Responsible for relevant security awareness training of employees
- Reviewing supplier information and cyber security standards and performing an analysis on potential gaps and risks
- Ensure vendors comply with group security requirements.

Essential Qualifications & Experience

- **Education:**
    - Bachelor's degree in computer science, Information Technology, Cybersecurity, or a related field.
    - Master's degree in Cybersecurity or a related field is highly preferred.
- **Certifications:**
    - Relevant industry certifications such as:
        - Certified Information Systems Security Professional (CISSP)
        - Certified Information Security Manager (CISM)
        - Certified Ethical Hacker (CEH)
        - CompTIA Security+
        - ISO 27001 Lead Implementer/Auditor
- **Experience:**
    - Minimum 5-7 years of experience in information security roles (e.g., Security Analyst, Security Engineer).
    - Proven experience in implementing and managing information security programs.
    - Hands-on experience with security tools and technologies (e.g., firewalls, intrusion detection systems, antivirus software, SIEM).