Case Study: Achieving SOC 2 & ISO 27001 Compliance at Rohlik.cz

**Introduction:**

Rohlik.cz, a leading online grocery retailer, aims to implement SOC 2 and ISO 27001 to enhance its information security and protect customer data. They recognize the critical role of secure software development in this process.

**Your Role:**

As an information security consultant with expertise in SOC 2, ISO 27001, and secure software development, you will guide Rohlik.cz through this compliance journey. You've already analyzed their current security practices and identified areas for improvement.

**Case Study Objectives:**

1. **Develop a Roadmap:** Create a detailed plan for achieving SOC 2 and ISO 27001 compliance, outlining steps, timelines, responsibilities, and milestones. Prioritize actions based on risk and business impact.
2. **Recommend Solutions:** Propose practical solutions to address security gaps, including technology choices and cost-benefit considerations. Develop a communication strategy to ensure smooth adoption of new security measures.
3. **Integrate Secure Software Development:**
   * Secure SDLC: Integrate security into every phase of the software development lifecycle (SDLC), from design to deployment.
   * Secure Coding: Establish and enforce coding standards to minimize vulnerabilities.
   * Vulnerability Management: Implement robust processes for identifying, assessing, and remediating software vulnerabilities.
   * Change Management: Ensure secure change control procedures for software updates.
   * Security Testing: Regularly perform security testing (e.g., penetration testing, code reviews) to identify and address potential risks.

**Additional Considerations:**

* How will compliance enhance customer trust and provide a competitive advantage?
* How can Rohlik.cz maintain ongoing compliance and adapt to evolving threats?
* How should Rohlik.cz prepare for and undergo a successful third-party audit?

**Deliverables:**

1. A comprehensive report detailing your findings, recommendations, and the implementation roadmap with a focus on secure software development.
2. A presentation to Rohlik.cz's management, summarizing key findings and proposed solutions.

**Challenge:**

This case study allows you to showcase your expertise in information security, risk management, and secure software development within a real-world context. Your solutions will directly contribute to Rohlik.cz's success in protecting customer data and achieving industry-recognized security standards.