**The main components of the Information Security Management System preparation:**

1. **CONTEXT ESTABLISHMENT** (Ustanowienie kontekstu)
   1. **Basic criteria**
      1. Risk evaluation criteria:
         1. The strategic value of the business information process
         2. The criticality of the information assets involved
         3. Legal and regulatory requirements, and contractual obligations
         4. Operational and business importance of availability, confidentiality and integrity
         5. Stakeholders expectations and perceptions, and negative consequences for good-will and reputation
      2. Impact criteria:
         1. Level of classification of the impacted information asset
         2. Breaches of information security (e.g., loss of confidentiality, integrity and availability)
         3. Impaired operations (internal or third parties)
         4. Loss of business and financial value
         5. Disruption of plans and deadlines
         6. Damage of reputation
         7. Breaches of legal, regulatory or contractual requirements
      3. Risk acceptance criteria:
         1. Business criteria
         2. Legal and regulatory aspects
         3. Operations
         4. Technology
         5. Finance
         6. Social and humanitarian factors
   2. **The scope and boundaries**
      1. Study of the organization
         1. The organization’s main purpose
         2. Its business
         3. Its mission
         4. Its values
         5. Structure of the organization
         6. Organization chart
         7. The organization’s strategy
      2. List of the constraints affecting the organization
      3. List of the legislative and regulatory references applicable to the organization
      4. List of the constraints affecting the scope
   3. **The organization for the information security risk management process**
2. **RISK ASSESSMENT** (Ocena ryzyka)
   1. **Risk analysis (which encompasses risk identification and risk estimation)** 
      1. Risk identification
         1. Identification of assets
         2. Identification of threats
         3. Identification of existing controls
         4. Identification of vulnerabilities
         5. Identification of consequences
      2. Risk estimation
   2. **Risk evaluation**
3. **RISK TREATMENT PLAN** (Plan postępowania z ryzykiem)
4. **RISK ACCEPTANCE STATEMENT** (Akceptacja ryzyka)
5. **RISK COMMUNICATION** and **RISK MONITORING AND REVIEW** (Komunikacja ryzyka) (Monitorowanie oraz przegląd ryzyka)