1. Context Establishment

2. Risk Assessment

2.1 Risk Identification

2.1.1 Setup basic criteria

2.1.2 Define approach

2.1.3 Define acceptance criteria

2.2 Risk Analysis

2.2.1 Identify assets

2.2.2 Identify threats

2.2.3 Identify controls

2.2.4 Identify vulnerabilities

2.2.5 Incident scenarios

2.3 Risk Evaluation

2.3.1 Evaluate risk

2.3.2 Select methodologies

2.3.3 Assess consequences

2.3.4 Assess controls likelihood

2.3.5 Determine level of risk

3. Risk Treatment

3.1 Treat risk

3.2 Avoid risk

3.3 Modify risk

3.4 Share risk

3.5 Return risk

4. Risk Acceptance

4.1 Accept risk

4.2 Rejected risk

5. Risk Monitoring & Review

5.1 Monitor & review risk

6. Risk Communication & Consultation

6.1 Communicate & consult risk

Description

Study of the organization
- Purpose, business, missions, values, strategies, structure
- Asset classification
- Primary assets, business process & activities, information
- Supporting assets: hardware, software, network, personnel, site, structure
- Constraints
  - Organization: political, cultural, personnel, strategical, territorial, economical, financial, structural, functional, timing, methodical etc.
  - Scope: non-existing processes, technical, financial, environmental constraints, time, methodical, organizational etc.
- Risk modification: time, financial, technical, operational, cultural, ethical, environmental, legal, ease of use, personnel, existing controls etc.

References