1. Risk management framework

- ☐ The scope and objectives of risk management are clarified.
- ☐ Policy for risk management has been developed.
- ☐ Responsibilities and roles are defined.

2. Identification of risks

- ☐ Internal and external risks are identified in accordance with the BSI Compendium.
- ☐ Identified risks are documented.

3. Assessment of risks

- ☐ The probability and potential impact of each risk are analysed.
- ☐ Qualitative and quantitative assessment techniques are used.
- ☐ Risks are prioritised based on their assessment.

4. Coping strategies

- ☐ Suitable measures for risk minimisation, avoidance or acceptance are identified.
- ☐ Emergency plans and risk minimisation strategies have been developed.
- ☐ Controls and measures are implemented.
- ☐ Residual risks after implementation of the measures are assessed and known to risk owners.

5. Communication

- ☐ All stakeholders are informed about identified risks and planned measures.
- ☐ Communication is demonstrably clear and understandable.
- ☐ Regular reporting and risk monitoring meetings are implemented.

6. Documentation

- ☐ All measures and their results are documented.
- ☐ Reports and analyses are recorded regularly.

7. Monitoring and review

- ☐ System for the continuous monitoring of risks has been implemented.
- ☐ Risk assessments and measures are regularly reviewed and updated
- ☐ Regular audits and reviews are carried out.

8. Training and sensitisation

- ☐ Employees are trained in dealing with risks and in the risk management process.
- ☐ Risk-conscious corporate culture is promoted.

9. Continuous improvement (PDCA)

- ☐ Feedback and lessons learnt are used to improve risk management.
- ☐ Processes and strategies are adapted to new developments and findings.