9. Performance Evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.2 Internal Audit

9.3 Management Review

9.1 Monitoring, Measurement, Analysis and Evaluation

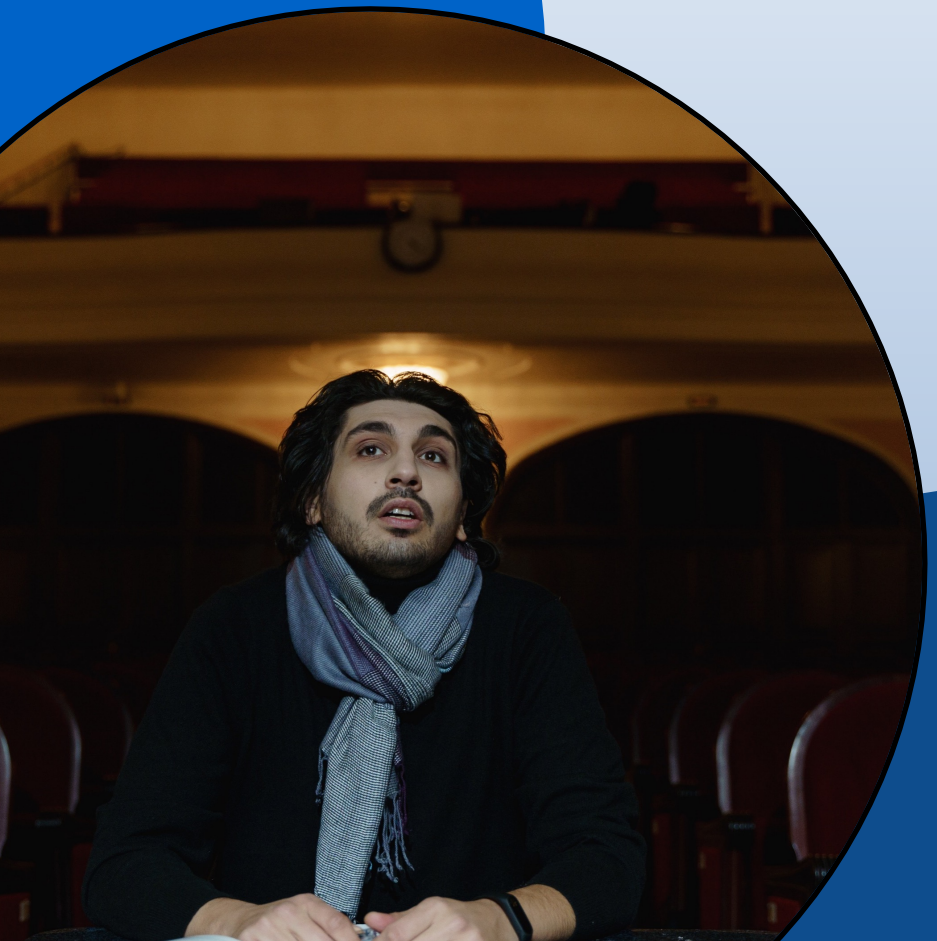
Organisation should provide

- **Metrics for the ISMS performance regarding**
  - **Compliance with standard**
  - **Alignment with policies**
  - **Achievement of objectives**
- **Take into consideration**
  - **What need to be monitored and measured**
  - **Methods of monitoring and measurement**
  - **Frequency to perform monitoring and evaluation**
  - **Who is responsible**
- **Performance results should be retained**

Examples of measurements

- Number of information security incidents
- Number of security breaches
- Duration of service interruption
- MTTRS : Meantime to restore service
- Number of security related downtimes
- Accomplishment of information security objectives

9.2 Internal Audit



- Performed at planned intervals
- Auditors should be independent
- Audit program should be documented
- Criteria and scope must be defined
- Non conformities should be reported
- Audit program and records should be retained

9.3 Management Review

- Must be done at planned interval
- Status of actions from previous reviews
- ISMS performance
  - Nonconformities and corrective actions
  - Monitoring and measurement results
  - Fulfillment of information security objectives
- Improvement opportunities
- Must be documented