10. Improvement

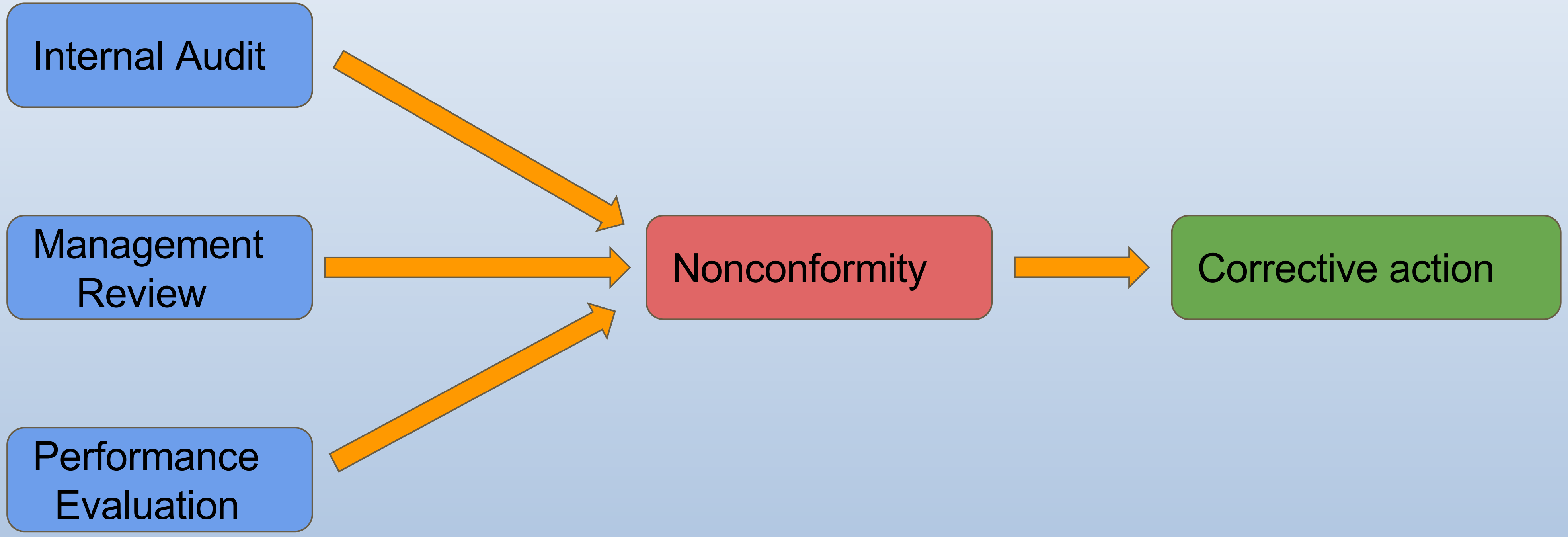
10.1 Nonconformity and corrective action

- Identify nonconformities in the ISMS
- Take corrective actions
- Keep records

10.2 Continual Improvement

- Improve the effectiveness of the ISMS
- Review the ISMS periodically

10.1 Nonconformity and corrective action



Examples of Nonconformities

- The failure to comply with clause 4.2.1 lack of defining the scope
- No ISMS policy,
- No risk assessment,
- Absence of statement of applicability
- Failure to comply with Clause 7: Management review of the ISMS.
- Failure to comply with the Internal ISMS audit (Clause 6)

10.1 Nonconformity and corrective action

In the event of nonconformity

- Take action to correct it
- Deal with the consequence
- Review effectiveness of corrective action
- Documentation

Evaluate the need for action to eliminate causes by

- Review of the nonconformity
- Determine the cause
- Determine if similar non conformity exist or may occur.

Example of corrective action

Nonconformity : 2 of 10 PCs have no antivirus installed

Corrective action : install antivirus on the 2 PCs

Cause : finance department buy its own PCs directly

Similar non conformities : check if any other departments are buying their PCs directly.

Root cause corrective action : set up a procurement process for PCs and enforce it.

10.2 Continual Improvement

Continual improvement is key to achieve and maintain

- Suitability
- Effectiveness of the ISMS