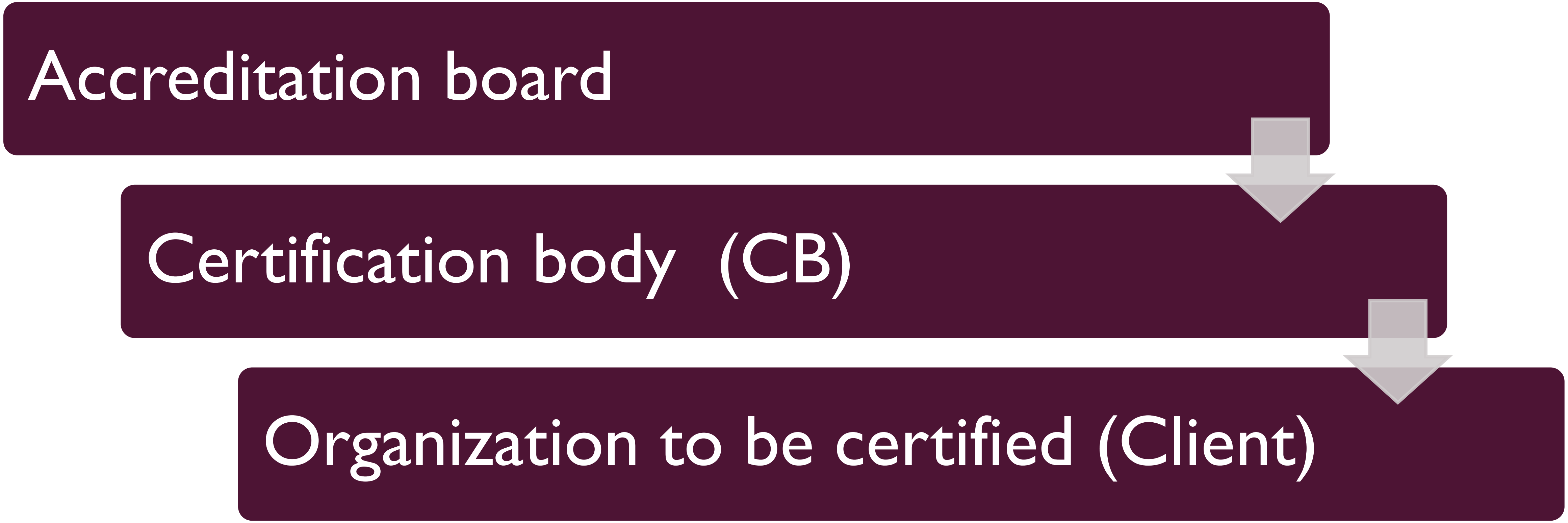
AUDITING ISO 27 001 BASED INFORMATION SECURITY MANAGEMENT SYSTEM

TIPS & TRICKS

ACCREDITATION PROCESS

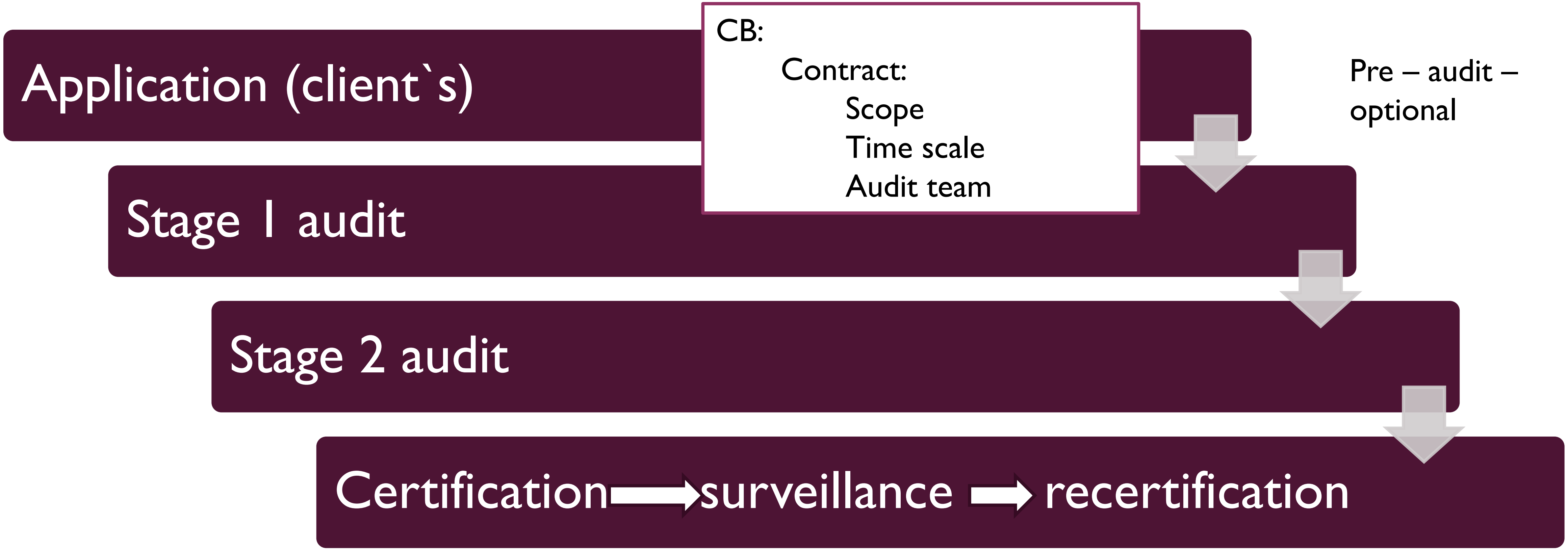


Accreditation board

Certification body (CB)

Organization to be certified (Client)

CERTIFICATION PROCESS



Application (client`s)

Stage I audit

Stage 2 audit

Certification → surveillance → recertification

CB:

Contract:

Scope

Time scale

Audit team

Pre – audit – optional

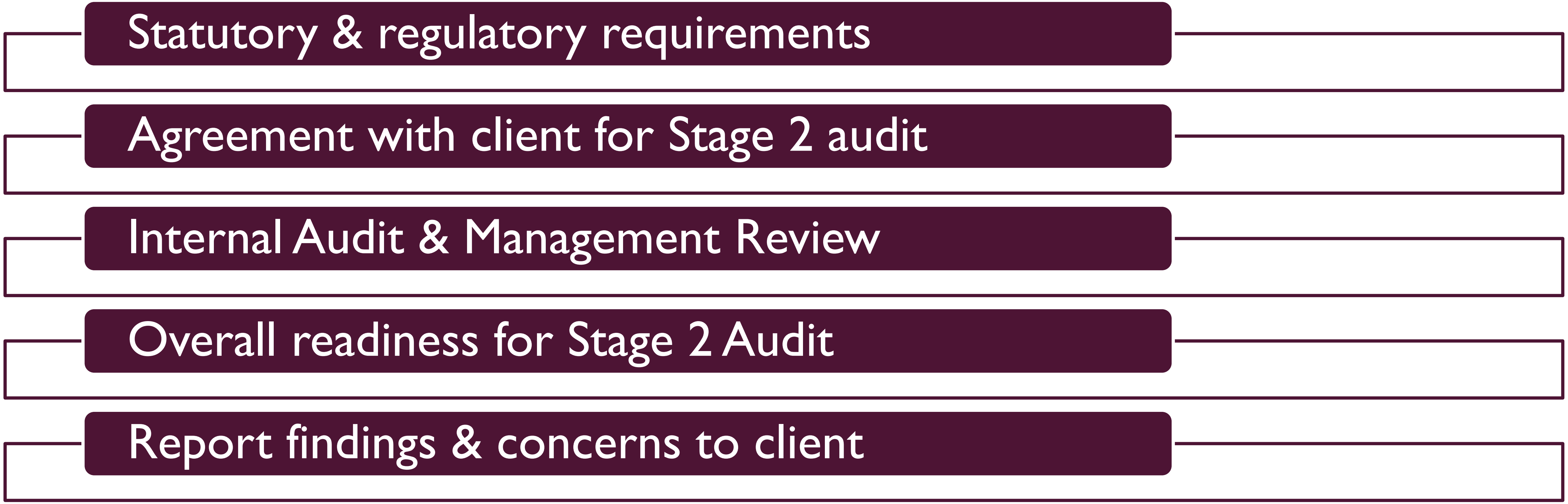
APPLICATION REVIEW

- Certification Body template
- Adequacy of INFO about client
- Does Certification Body have the competence

STAGE I AUDIT

- Onsite recommended
- Documentation
- Evaluation of location / site specific conditions
- Review of key performance parameters
- Validation of scope

STAGE I AUDIT



- Statutory & regulatory requirements
- Agreement with client for Stage 2 audit
- Internal Audit & Management Review
- Overall readiness for Stage 2 Audit
- Report findings & concerns to client

STAGE 2 AUDIT

- Policies, procedures, achievement of objectives
- Overall information security management system effectiveness
- Compliance with 27 001 requirements
- Onsite - MUST

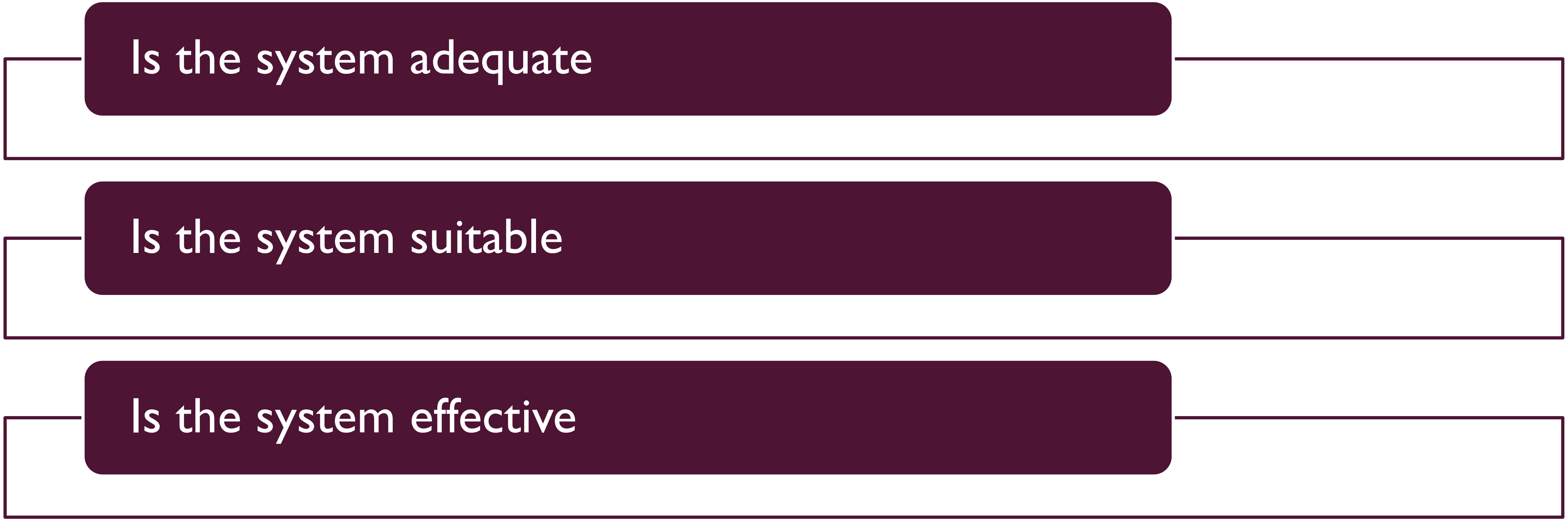
STAGE 2 AUDIT

- Risk assessment
- Selection & implementation of controls based on Risk Assessment
- Monitoring, measurement, analyses
- Internal Audit & Management Review
- ! Link among controls, Statement Of Applicability, Risk Assessment results, policy & objectives

STAGE 2 AUDIT

- Link among statutory & regulatory requirements, policy, objectives & targets
- Corrective Actions
- Continual improvement

STAGE 2 KEY «?»



Is the system adequate

Is the system suitable

Is the system effective

SURVEILLANCE AUDITS

½ / once a year

All processes / functions covered in 3 years

Audit plan based on previous audit results, Internal Audit

GOOD AUDIT

- Lead auditor has overall responsibility
- Planning & preparation
- Communication (client, auditees, auditors)
- Accurate & objective fact finding

ROLES

- Auditee
- Guide
- Audit client
- Observer

AUDIT TYPES

- 1st party - self
- 2nd party – by interested body
- 3rd party – Certification Body

AUDIT METHODS ON SITE HUMAN INTERACTION

- Interviews
- Checklists
- Document review
- Sampling

AUDIT METHODS ON SITE NO HUMAN INTERACTION

- Document review
- observations
- On site visits
- Check lists
- Sampling

AUDIT METHODS OFF SITE HUMAN INTERACTION

- Remote interviews
- Remote checklists
- Remote document review

AUDIT METHODS OFF SITE NO HUMAN INTERACTION

- Document review
- Remote observations
- Data analyses

AUDIT CRITERIA

- Standard
- Contractual specifications
- Information security management system documentation
- Information security management system planning
- Legislation

AUDIT SCOPE

Location

Organisational units

Activities & processes covered

AUDIT PLAN

- Scope

Shifts MUST BE COVERED!

- Criteria
- Dates & duration
- Audit team

WORKING DOCUMENTS

- Checklist
- Forms
- Standard
- Guidelines

ON SITE AUDIT ACTIVITIES

- Opening meeting
- Communication during audit
- Collecting & verifying information
- Preparation of conclusions
- Closing meeting

Seeing is believing!

CHECK LISTS

- Specific
- Note documents to review
- Identify records to sample
- Key people to interview
- Key «?»

OPENING MEETING

- Team introduction
- Scope & criteria
- Plan & methods
- Sampling
- Confidentiality

CLOSING MEETING

- Thanks
- Report + & - observations
- Questions & Answers
- Corrective actions (eliminate the cause) & timescale
- Recommendation

NC is a field for improvement!
Always evidence!

FOLLOW UP

- At agreed time
- Review of document evidence
- Re audit onsite – only corrective action! Only

Documentary evidence:

- Records
- Training certificates
- Amended procedures
- Photos
- Video