

## The Ultimate Checklist for an ISO 27001 Certification Audit

### **Before the Engagement Starts:**

- ISMS is fully documented and up-to-date.
- Required policies and procedures are in place and being followed.
- Risk assessment is current and all identified risks have been addressed through appropriate controls.
- All key processes have been identified and documented.
- All required records are in place and up-to-date.
- Employees within scope are aware of their roles and responsibilities.
- Necessary training has been provided to employees on their responsibilities related to the ISMS.
- Monitoring and measurement activities are being performed as required and producing accurate results.
- Security controls are in place and operating effectively.
- Review all previous audit reports and ensure that corrective actions have been completed (if applicable).
- Assess all changes in activities and take action (if applicable).

**During the Engagement:**

- Communication channel between auditor and all relevant personnel is opened.
- Audit schedule is up-to-date.
- Audit is scheduled internally as early as feasible.
- Employees who will be interviewed by the auditor are prepared and know what to expect.
- All employees are aware of the audit and understand their role in supporting it.
- Necessary documentation is available and easily accessible to the auditor.
- Audit findings and recommendations are documented and tracked to closure.
- Don't Panic! once the audit starts.

**After the Engagement:**

- Final audit report accurately reflects the current state of your ISMS.
- All non-conformities have been addressed and corrective actions have been planned.
- All recommendations made by the auditor have been addressed.
- All necessary follow-up actions have been completed and documented.
- Periodic reviews to ensure ongoing compliance with the ISO 27001 standard are scheduled