ISO 22301 Checklist

A simple checklist to make sure your ISO 22301 Implementation hits on the key points of the attestation.

Business Impact Analysis (BIA)
Determining recovery requirements

- Identify all functions performed for all departments within scope.
- Map interdependencies and information flows between functions to fully understand the consequences of loss.
- Determine the length of time that the organization can live without each function before the loss becomes unacceptable (e.g., Recovery Time Objectives [RTOs]).
  
  (look beyond loss of revenue as the sole criterion).
- Identify enabling requirements (IT, personnel skill sets, etc.).
- Validate frequency of backups.
- Identify Single Points of Failure (SPOFs).

Recovery Strategy Analysis (RSA)
Understanding and fulfilling recovery requirements

- Develop your recovery organization with the necessary teams and their proper staffing.
- Understand the available recovery strategies in the industry and the Recovery Time Objectives (RTOs) those strategies support.
- Map requirements from the BIA to the available strategies, determine cost and ease of implementation and then decide the best strategies for your organization.
- Implement the necessary contracts and integrate those strategies into your recovery solution.
**Business Continuity Plan (BCP)**

Write your plans to include the following:

- Damage assessment procedures.
- Activation criteria based on the comparison between the estimated time to repair and RTOs.
- Recovery team(s) rosters and sub-plans for those teams that provide the activation procedures for the approved strategies.
- Critical vendor / supplier POCs and contact information.

**BCP Training**

**Develop critical skills**

- Ensure your people with recovery roles and responsibilities are trained to fulfill those duties.
- Ensure all personnel in the organization have a familiarization of recovery policies and where to go for information in the event of an incident / disaster.

**Exercise Your Plan**

**Test to verify your plans efficacy**

- Use realistic scenarios.
- Ensure coordination and participation among all personnel with recovery roles and responsibilities.
- Use the exercise results to refine your plan and update training curriculum.

If you have any questions or would like to speak with an ISO 22301 expert, reach out!

ISO22301@pivotpointsecurity.com

Where to turn... when ISO 22301 matters