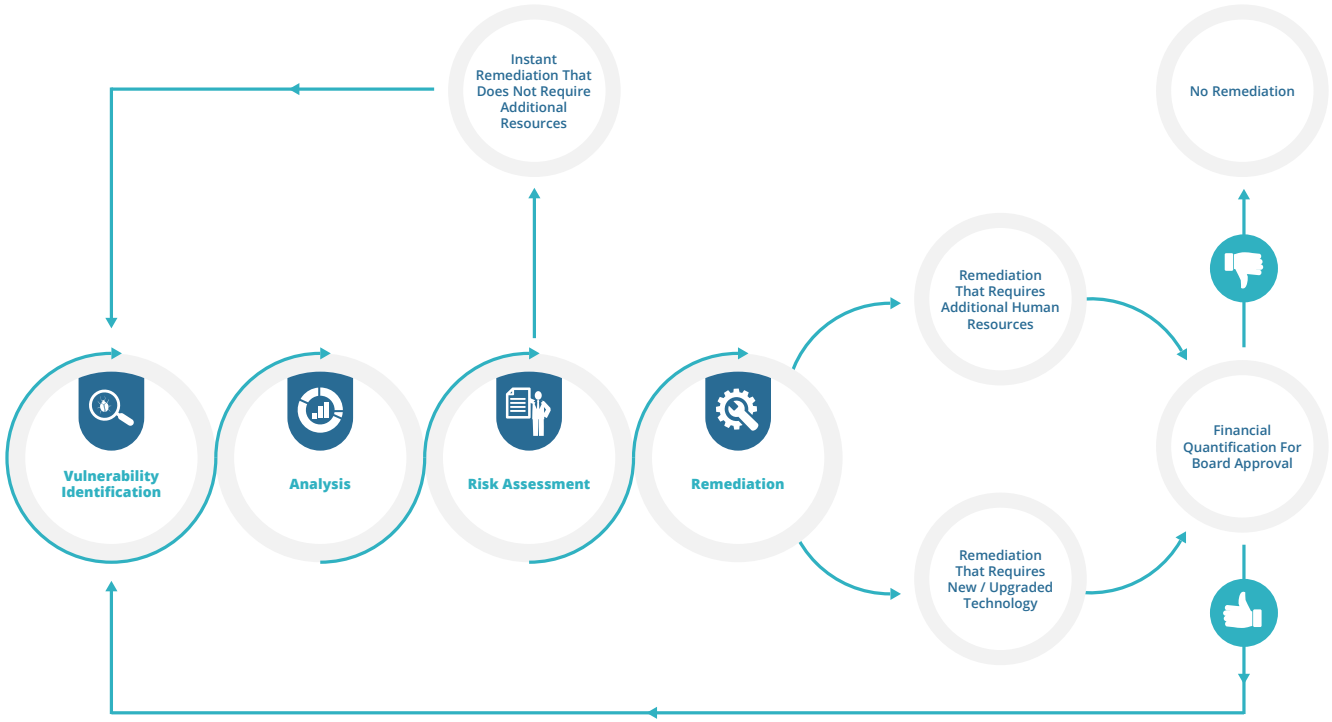
In collaboration by:

Boardish

360° inControl
FIRST CHOICE IN BUSINESS EXCELLENCE

Best Practice Business Vulnerability Assessment Process



Phase 1: **Initial Identification, Assessment, And Instant Remediation**

Step 1: Vulnerability Identification – Including manual, automatic or hybrid solutions.

Step 2: Analysis - Understanding the vulnerabilities and "cleaning" false positives.

Step 3: Risk Assessment – Putting all your vulnerabilities in a risk framework and providing clear risk-based priorities. You can fix risks immediately without additional resources in this step.

Step 4: Remediation – Creating a remediation plan to fix your vulnerabilities.

Phase 2: **Planning Necessary Resources**

Step 5: Solutions - Including new hardware and software technology in your remediation plan.

Step 6: Experts - Discovering and including additional human resources (internal or outsourced) in your remediation plan.

Step 7: Quantification - Quantifying the remediation plan into financial figures for your decision-makers.

Phase 3: **Taking The Quantification To Decision-Makers**

Outcome: Budget request approved – Implement remediation of the vulnerability.

Outcome: Budget request denied – Decision-makers take responsibility for the vulnerability.